A RISK BASED APPROACH FOR MANAGING INFORMATION TECHNOLOGY SECURITY RISK WITHIN A DYNAMIC ENVIRONMENT

by

NTOMBIZODWA BESSY MAHOPO

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor:	MISS H. ABDULLA
Co-Supervisor:	MR M. MUJINGA

November 2015

DECLARATION FORM

DECLARATION

Student Number: 49020056

I declare that *A Risk Based Approach For Managing Information Technology Security Risk Within A Dynamic Environment* is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I have not previously submitted this work, or part of it, for examination at UNISA for another qualification or at any other higher education institution.

Signature: 

Date: 03/09/2015

DEDICATION

I dedicate this dissertation to my daughter **Onalerona Mahopo** and my son **Rorisang Mahopo.**

ACKNOWLEDGEMENTS

First, I would like to thank God for blessing me with His divine wisdom and being with me throughout this journey and beyond.

I would like to express my gratitude to the following people:

- My husband, **Greaves Mahopo,** for always loving me, supporting me and believing in me.
- My children, **Ona and Rori,** for always giving me a reason to continue working hard. You are the light in mommy's life!
- My parents, **Simon Gomba and Annah Gomba,** for your unconditional love and for raising me to be the woman that I am today. Dad, you always reminded me of the importance of education from as far back as I can remember. Mom, you always offered me your words of encouragement throughout this journey and looked after the kids on weekends when I could not.
- My study buddies, **Precious Gomba and Rudy Bopape,** for sharing the vision and excitement for this dissertation, for walking each step of this journey with me, for always being available to listen to my frustrations when studying seemed like a high mountain to climb, and for always helping me focus on the end goal. You guys are a great inspiration in my life. I have no doubt that both of you will also finish your dissertations.
- My sisters, **Carol, Precious and Keabetswe;** my mother-in-law, **Seeifo;** and the rest of my family and friends, for being my number one supporters always…
- My supervisors, for your academic guidance.

Thank you… This awesome adventure has eventually ended!

ABSTRACT

Information technology (IT) security, which is concerned with protecting the confidentiality, integrity and availability of information technology assets, inherently possesses a significant amount of known and unknown risks. The need to manage IT security risk is regarded as an important aspect in the daily operations within organisations. IT security risk management has gained considerable attention over the past decade due to the collapse of some large organisations in the world.

Previous investigative research in the field of IT security has indicated that despite the efforts that organisations use to reduce IT security risks, the trend of IT security attacks is still increasing. One of the contributing factors to poor management of IT security risk is attributed to the fact that IT security risk management is often left to the technical security technologists who do not necessarily employ formal risk management tools and reasoning. For this reason, organisations find themselves in a position where they do not have the correct approach to identify, assess and treat IT security risks.

The IT security discipline is complex in nature and requires specialised skills. Organisations generally struggle to find a combination of IT security and risk management skills in corporate markets. The scarcity of skills leaves organisations with either IT security technologists who do not apply risk management principles to manage IT security risk or risk management specialists who do not understand IT security in order to manage IT security risk.

Furthermore, IT is dynamic in nature and introduces new threats and vulnerabilities as it evolves. Taking a look at the development of personal computers over the past 20 years is indicative of how change has been constant in this field, from big desktop computers to small mobile computing devices found today. The requirement to protect IT against threats associated with desktops was far less than the requirement associated with protecting mobile devices. There is pressure for organisations to ensure that they stay abreast with the current technology and associated risks.

Failure to understand and manage IT security risk is often cited as a major cause of concern within most organisations' IT environments because comprehensive

approaches to identify, assess and treat IT security risk are not consistently applied. This is due to the fact that the trend of IT security attacks across the globe is on the increase, resulting in gaps when managing IT security risk.

Employing a formal risk based approach in managing IT security risk ensures that risks of importance to an organisation are accounted for and receive the correct level of attention. Defining an approach of how IT security risk is managed should be seen as a fundamental task and is the basis of this research.

This study aims to contribute to the field of IT security by developing an approach that assists organisations in treating IT security risk more effectively. This is achieved through the use of a combination of existing best practice IT security frameworks and standards principles, basic risk management principles, as well as existing threat modelling processes.

The approach developed in this study serves to encourage formal IT security risk management practices within organisations to ensure that IT security risk is accounted for by senior leadership. Furthermore, the approach is anticipated to be more proactive and iterative in nature to ensure that external factors that influence the increasing trend of IT security threats within the IT environment are acknowledged by organisations as technology evolves.

Keywords: IT, IT security, risk, risk management, IT security threat modelling, IT security risk management, OCTAVE, COBIT, ITIL, ISO 27001/2, ISF Standard of Good Practice

DEFINITION OF TERMS

This table provides definitions of the significant terms, abbreviations and acronyms used in this document.

Table A – Definition of Terms

#	KEY TERM/ACRONYM	DESCRIPTION
1	IT	Information Technology (IT) is a set of people, processes and technology that allows information to be input, processed, output and stored throughout the information life cycle (Stoneburner, Goguen & Feringa, 2002)
2	IT asset	A resource that has high value, such as information or a file system (Swiderski & Snyder, 2004).
3	Risk	A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities and that may be avoided through pre-emptive action (ISO/IEC31001, 2009).
4	Risk management	The identification, analysis, assessment, control, avoidance, minimisation, or elimination of risk (ISO/IEC31001, 2009).
5	Risk management framework	A risk management framework is a structure used to identify initiating events and the event sequences that might contribute significantly to risk. It provides realistic quantitative measures of the likelihood and the impact should the risk materialise, thereafter providing guidance on how that risk should be treated (ISO/IEC31001, 2009).
6	IT security	The process of safeguarding an organisation's data and systems from unauthorised access or modification to ensure its availability, confidentiality and integrity (Ajibuwa, 2008).
7	IT security threat	A potential danger that might exploit a vulnerability and cause harm to an IT asset (Myagmar, Lee & Yurcik, 2005).
8	IT security attack	An IT security attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an IT asset (Jouini, Rabai & Aissa, 2014).
9	IT security vulnerability	Vulnerability is a weakness within an IT asset which allows an attacker to compromise the IT asset (Jouini, et al., 2014).

PUBLICATIONS

The final deliverable of this study, the ITSRB approach, was presented and published in a peer-reviewed conference at the Information Security South Africa Conference 2015.

1. Mahopo B., Abdullah H. & Mujinga M, 2015 August, *A formal qualitative risk management approach for IT security*, Proceedings of the 2015 Information Security for South Africa Conference, IEEE Catalog CFP1566I-CDR, ISBN 978-1-4799-7754-3.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

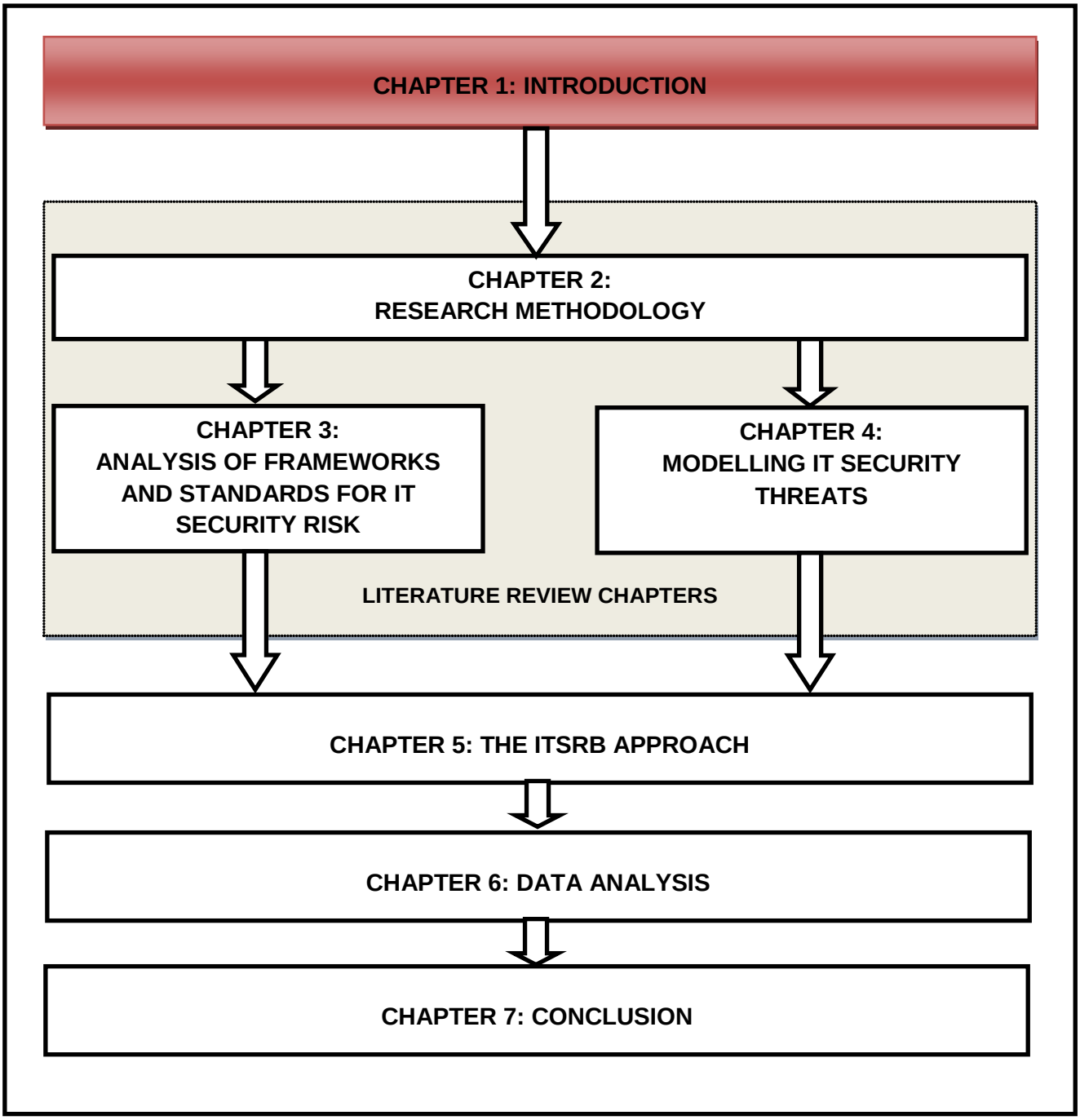

Figure 1.1 – Dissertation Layout: Chapter 1

1.1. INTRODUCTION

The rapid growth of society's dependence on Information Technology (IT) has precipitated increasing dedication to IT security (Bhasker & Kapoor, 2009). Organisations and individuals always find themselves under pressure to stay abreast with the current technology in order to run their businesses or their lives, whereby their IT systems are open to the Internet (Krichene, 2008). There is a tremendous amount of innovation involved with technology, which introduces a great deal of complexity within the IT environment, thus resulting in a significant number of IT security risks (Ketel, 2008). IT security is a complex topic and evolves almost as fast as technology does (Kolias, Stavrou, Voas, Bojanova & Kuhn, 2016).

While research in IT security has begun to draw attention to the importance of IT security risk management, the focus is still on the development of procedural guidelines and a few semi-automated methods (Chorppath & Alpcan, 2012). Several issues remain unsolved including the need for sophisticated formalisation in risk management reasoning (Krichene, 2008), which forms the basis of this study. With the foregoing in mind, the main objective of this study is to investigate if existing IT security frameworks and standards and risk management principles within the best practice body of knowledge can be extended to increasingly enhance management of IT security risk.

1.2. BACKGROUND AND MOTIVATION

A risk management process is required to identify, describe and analyse possible vulnerabilities that could affect organisations' assets (Ajibuwa, 2008). Risk management is an iterative process that should lead to continuous improvement in an organisation's risk posture (Kolias, et al., 2016).

For organisations to mitigate IT security risk, there should be measures that are implemented to minimise the likelihood and impact of risk, namely, controls (Burns, 2005). Since the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management to use the least-cost approach to implement prioritised controls (Alberts, et al., 2003). The implementation of prioritised controls assists to decrease risk to an acceptable level, with minimal

adverse impact on the organisation's resources and mission (Ketel, 2008; Krichene, 2008).

Klemen and Biffl (2004) state that over time, a number of specific risk management approaches have been developed, including IT security risk management. IT security risk management is described as the process for the detection, reaction, and reflection procedures for IT security incidents (Amoroso, 1994; Klemen & Biffl, 2004). IT security risk management should be practised within organisations in order to achieve the goal of protecting IT and managing the associated risk (Chorppath & Alpcan, 2012). Having discussed the background to IT security risk management, the motivating factors that prompted this study are presented in the following sections.

7.4.1. Increasing trend of IT security attacks

Previous investigative research within the field of IT security in recent years have indicated that despite the efforts that organisations employ to reduce IT security risks, the trend of IT security attacks is still increasing (Netland, 2008; Straub, 2011). The window of time between the disclosure of a new vulnerability as well as the emergence of unique threats that operate against these new vulnerabilities continues to increase (Roos, 2008; Foley, 2009; Walser, et al., 2009). The volume of unknown IT security attacks is increasing, and as a consequence, the potential impact also increases (Roos, 2008).

IT security attacks are still being launched against known vulnerabilities which organisations tend to ignore until they are exploited by hackers, resulting in less focus on unknown threats and vulnerabilities (Nakrem, 2007). Ogut (2006) attests that the scale and scope of hacker and virus attacks on computer systems are on the rise because recurring security breaches have increased.

The fact that information systems are open to the Internet and the scale of hackers and viruses on information systems is increasing indicates that there is still a gap in managing IT security risk (Kolias, et al., 2016). Extending the risk management processes to provide insight to known and unknown threats as well as provide a real-time holistic threat management solution is an area that requires attention (Krichene,

2008).The subsistence of this problem insinuates that reactive methods for addressing IT security attacks are still being employed within organisations. This statement prompts the motivating factor that follows.

7.4.2. Poor risk management practices

Failure to understand, identify and manage risk is often cited as a major cause of IT problems (Obrand, et al., 2012). Business executives often do not understand the environment in which the IT security function operates and what questions they should be asking their IT security personnel, resulting in a barrier to effective communication (Reid & Gilbert, 2007). Incomplete knowledge about the IT security domain in general and the current IT security status of the organisation is one of the main problems in IT security risk management (Fenz & Ekelhart, 2009).

Van der Leeden (2010) conducted a study that indicate that despite the application of various risk management frameworks and standards into mitigating IT security risks, there is still a gap in dealing with both known and unknown IT security attacks. The unfortunate fact is that most risk management methodologies available in the marketplace are reactive in nature and as a consequence end up neglecting to cater for unknown threats (Chorppath & Alpcan, 2012). Both known and unknown threats still remain a great IT security challenge for organisations (Van der Leeden, 2010; Kolias, et al., 2016).

Ogut (2006) states that organisations use financial instruments such as insurance to hedge losses resulting from IT security breaches. Even though these financial and technological instruments reduce security vulnerabilities and losses from IT security breaches, it is not clear how organisations should manage their IT security risk (Ogut, 2006).

The major reason behind the use of financial instruments to hedge IT security losses is that organisations seldom trust their IT security practitioners (Ponenti, 2008).. Organisations seldom trust their IT security practitioners because they are not objective about the process of implementing IT security controls; instead, they often rely on their intuition (Krichene, 2008). Unfortunately, this is the case because even the best practice IT security risk management frameworks and standards do not

provide adequate information for effective risk management (Kolias, et al., 2016). More specifically, most traditional IT security risk management processes ultimately boil down to only vulnerability identification for identifying a list of system vulnerabilities (Poolsappasit, 2010). Given the complexity of today's IT infrastructure, it is not enough to consider the presence or absence of vulnerabilities in isolation (Poolsappasit, 2010).

No single risk management framework is perfect or perfectly applicable to IT security (Ponenti, 2008). Non-existence of an IT security risk management framework leaves the decision-makers (i.e. IT security practitioners) with a series of challenges, the most pressing of which is to manage IT security risk in the ever-evolving arena of IT (Chorppath & Alpcan, 2012). It is therefore worth acknowledging that there is still ambiguity in the application of risk management within the field of IT security. This problem leads to the next motivating factor of this study.

7.4.3. The incomplete mitigation of IT security risk

Organisations employ security technologies such as firewalls, intrusion detection systems (IDS), encryption, biometric systems and other authentication systems to protect themselves against IT security attacks (Ogut, 2006). However, complete prevention of IT security breaches is technologically impossible and prohibitively expensive (Klemen & Biffl, 2004; Reid & Gilbert, 2007).

Despite the increasing interest of many researchers in developing IT security networks technologies and strengthening the existing approaches, IT security mechanisms are seldom applied with efficiency to the real world (Krichene, 2008). Computer systems and networks have become too complex to be addressed using formal proofs of computability and they make up the environment in which IT security mechanisms are deployed and adversaries attack (Schechter, 2004). The discipline of IT security risk management is still unable to answer satisfactorily the question of how much is enough as well as how much value is derived versus benefit realised (Soo Hoo, 2000; Arora, Hall, Piato, Ramsey & Telang, 2004)). Ogut (2006) raises a valuable point by stating that even though the financial and technological controls reduce security vulnerabilities to a certain level, it is still not clear how organisations should proactively manage IT security risk.

1.3. PROBLEM STATEMENT

Various authors (Ogut, 2006; Krichene, 2008; Ajibuwa, 2008) illustrate in their studies that IT security risk management has proven to be a challenging task because to date, organisations still suffer from IT security attacks on both known and unknown vulnerabilities. The trend of IT security threats is on the increase, as IT security specialists are still reactive in counteracting against the community of malicious hackers and do not place high focus on becoming more proactive (Straub, 2011). The proliferation of IT has made the world seem much smaller, as computer-related innovations, such as the Internet, allow individuals on opposite sides of the world to interact in ways that were unimaginable a few decades ago (Krichene, 2008). Straub (2011) highlights that the deliberate and opportunistic paths of IT security compromise emanate from the Internet and attract hackers in that manner.

On the other hand, formalisation in the risk management reasoning within the field of IT security is poor (Krichene, 2008). Fenz and Ekelhart (2009) express that incomplete knowledge about IT security and the IT security status of the organisation is one of the main problems in IT security risk management. The risk management frameworks and standards available in the body of knowledge do not support the complete process of risk management within the IT security environment (Krichene, 2008; Straub, 2011). In fact, unknown IT security attacks are quickly becoming the next great IT security challenge for today's organisations (Kolias, et al., 2016).

1.4. RESEARCH VALUE

This study is conducted through an exploratory exercise which analyses industry best practice IT security risk management frameworks and standards to assess if they can be extended to proactively manage IT security risk more effectively. By following the formal research methodologies, the target audience will have the opportunity to observe how they can use the proposed approach in their organisations to reduce the response rate to both known and unknown IT security attacks and the resulting risks. The research will be of value to any organisation's IT security environment, especially senior specialists within this field.

1.5. RESEARCH OBJECTIVES AND RESEARCH QUESTIONS

*The **main objective** of this study is to investigate whether strong characteristics of the existing IT security frameworks and standards, the basic risk management principles, as well as the IT security threat modelling processes within the best practice body of knowledge can be extended to develop a formal and proactive approach to managing IT security risk*.

*The **main research** question of this study is: "Can a formal, dynamic and proactive approach for managing IT security risk be developed through the use of existing IT security frameworks and standards, basic risk management principles and IT security threat modelling processes?"* The main objective is explored by investigating the sub-objectives and research questions that follow.

1.5.1. Research sub-objective 1

Research sub-objective 1**:** *Investigate the best practice IT security frameworks and standards which are most commonly used within financial institutions in South Africa by identifying their common characteristics and limitations.* This research sub-objective will be explored in Chapter 3. This sub-objective is explored by asking research question 1.

Research question 1: *Do the selected best practice IT security frameworks and standards most commonly used within the financial institutions in South Africa assist in managing IT security risk?*

1.5.2. Research sub-objective 2

Research sub-objective 2: *Investigate basic risk management principles and IT security threat modelling processes to assess their benefits for IT security risk management.* This research sub-objective will be explored in Chapters 3 and 4. This sub-objective is explored by asking research question 2.

Research question 2: *Can best practice risk management principles and IT security threat modelling processes be adopted for IT security risk management?*

1.5.3. Research sub-objective 3

Research sub-objective 3: *Consolidate the strong characteristics of the investigated IT security frameworks and standards, basic risk management principles, as well as IT security threat modelling processes to develop characteristics and attributes of a dynamic IT security risk management approach.* This research objective will be explored in Chapters 5 and 6. Furthermore, the sub-objective is explored by asking research question 3.

Research question 3: *Do the characteristics and attributes deduced from the investigated IT security frameworks and standards, risk management principles, and IT security threat modelling processes provide a good base for a proactive and dynamic IT security risk management approach?*

1.6. SCOPE AND LIMITATIONS

The objective of this study is achieved through the development of a holistic approach from the existing body of knowledge to assist professionals in the field of IT security to proactively manage IT security risk more effectively. The target audience for this study is limited to IT security professionals within the field of IT security.

The research sample in this study is limited to financial institutions within South Africa. This is due to the fact that financial institutions are particularly dynamic in nature because they enhance process efficiency and expand their business areas on a more regular basis (Maphakela, 2008). In addition to this, the repercussions of not dealing with IT security risk within financial institutions are much greater (Ajibuwa, 2008).

Common threat sources as explained by Stoneburner, et al. (2002) are natural threats, human threats and environmental threats. The intention of natural threats and environmental threats is not malicious; on that account, more attention is given to human threats, as the majority of malicious intentions in IT security emanate from them (Alhabeeb, et al., 2010). For the purpose of this study, only human threats are

focused on. Human threats are events that are either enabled by or caused by human beings (Stoneburner, et al., 2002). Examples include unintentional acts such as advertent data entry or deliberate actions such as network-based attacks, malicious software upload and unauthorised access to confidential information (Stoneburner, et al., 2002).

1.7. DISSERTATION LAYOUT

This dissertation is divided into seven chapters, with each chapter discussing differing aspects pertaining to this study. The dissertation layout is depicted in Figure 1.1.

Chapter 1: This chapter provides the introduction to the study. The background information, statement of the problem, research value, research objectives, scope and limitations of this study are discussed.

Literature Review Chapters

Chapters 2, 3 and 4 are categorised under literature review chapters as their content is based on theoretical literature found in the body of knowledge.

Chapter 2: This chapter presents the research methodology used to conduct this study by exploring existing literature. Additionally, the research strategy (i.e. survey) which is carried out for this study is presented, including the survey's development process.

Chapter 3: This chapter provides the literature review of the basic risk management principles as well as the existing IT security frameworks and standards, with the objective of deducing strong characteristics which can be used for managing IT security risk. The result of this chapter forms the theoretical basis of this study.

Chapter 4: This chapter focuses on the pragmatic processes of modelling IT security threats with the objective of demonstrating how threats can be treated before they manifest in materialised risks.

Chapter 5: This chapter presents the proposed IT Security Risk Based (ITSRB) approach which utilises the basic principles of risk management, IT security frameworks and standards, and the threat modelling processes using Chapters 3 and 4 as a theoretical foundation.

End of Literature Review Chapters

Chapter 6: The data collected from the survey (i.e. Chapter 6) is presented, and thereafter, the findings of the survey are analysed against the principles used to define the ITSRB approach.

Chapter 7: This chapter concludes this study by providing the summary of the findings as well as assess if the stated research objectives in Chapter 1 are met. This chapter concludes by outlining the significance of the contribution to the field of IT security. Recommendations for future research are also discussed in this chapter.

1.8. CONCLUSION

The field of IT security requires a formal approach to proactively manage risk within the IT environment. This chapter highlighted the need for conducting this study in order to assist organisations to manage IT security risk better through the use of basic risk management principles, IT security frameworks and standards, as well as threat modelling processes found in the existing body of knowledge. The background and motivation, research objective, research value, the scope and limitations of this study were presented to provide the context for the research.

The following chapter discusses the research methodology that is carried out by presenting the research strategy, methods and data collection tools used in this study.

2. RESEARCH METHODOLOGY

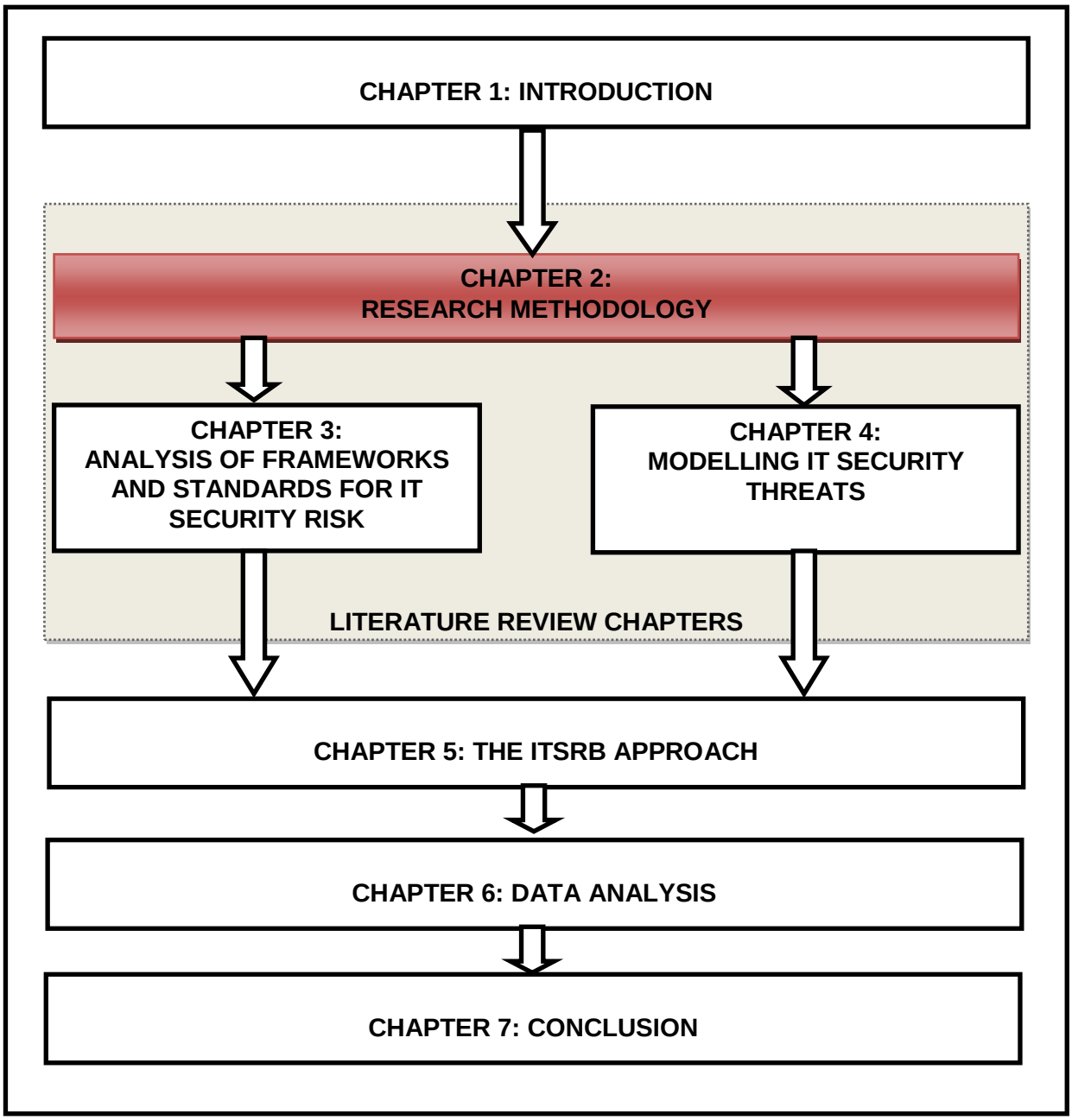

Figure 2.1 Dissertation Layout Chapter 2

2.1. INTRODUCTION

The preceding chapter provided an introduction and background to this study. The objective of this chapter is to present the research methodology that is used in this study. The background theory for the research methodology, with emphasis on the purpose of why this study is conducted, is presented. The selection of the research strategy is presented to provide the background for data requirements, the data generation method and the data analysis technique used to make conclusions.

The selected research strategy chosen, the process of gathering and analysing the data and the process of formulating the theory for this study are discussed in section 2.2. In addition to that, the reason for selecting quantitative measurement for data analysis is discussed in the same section (i.e. section 2.2). Section 2.3 includes the data collection process which is executed as part of the research methodology. This chapter is concluded in section 2.4.

2.2. RESEARCH METHODOLOGY

In common terms, research refers to a creation of new knowledge through the use of a robust process that aims to satisfy the people who will use the discovered results (Sivasubramaniyan, 2012). Research can also be defined as a scientific and systematic search of information on a specific subject (Rajasekar, Philominathan & Chinnathambi, 2013). The process of research consists of identifying a problem; formulating a theory; collecting, organising and evaluating data; and making deductions, suggesting solutions and reaching conclusions (Dawson, 2002; Oates, 2006; Sivasubramaniyan, 2012; Rajasekar, et al., 2013). To reach conclusions, the results must be carefully tested in order to determine whether or not they fit the formulating theory (Dawson, 2002).

A research methodology is a mode of systematically solving a research problem (Dawson, 2002; Krauss, 2005; Oates, 2006; Rajasekar, et al., 2013). A research methodology is concerned with the explanation of why a particular study is undertaken; how the research problem was formulated; which strategy is employed to carry out the research; what types of data is collected; and why a specific technique of data analysis is used (Krauss, 2005).

The two main classes of research are basic research and applied research (Rajasekar, et al., 2013). Basic research investigates the elementary principles and reasons for the occurrence of a particular event or phenomenon, whereas applied research solves certain problems using well known and accepted theories and principles (Oates, 2006). This study employs the principles of applied research because it uses foundational theories derived from existing IT security, risk management, and threat modelling frameworks and standards.

2.2.1. Six Ps of research

To describe the research methodology undertaken for this study, the 6Ps of research suggested by Oates (2006) were considered, namely, purpose, products, process, participants, paradigm and presentation.

2.2.1.1. Purpose: reason for conducting this research

This study is undertaken because literature revealed that there were gaps in the application of formal risk management in the field of IT security. This gap was also suggested as an area for future research (Krichene, 2008). This study therefore aims to propose the ITSRB approach that intends to address the identified gaps.

2.2.1.2. Product: outcomes of the research

To bridge gaps that exist in managing IT security risk, this study develops an approach through the use of strong characteristics extracted out of existing best practice frameworks and standards. The development process of the ITSRB approach is presented in the form of a framework.

2.2.1.3. Process: sequence of activities

To formulate the research problem, existing literature within the body of knowledge was investigated. The outcome of the investigation indicated that there is still a gap in how IT security risk is managed within organisations. The research objective was formulated based on the research problem, and the background and motivation. Thereafter, the research paradigm, the research strategy, the data generation

method, as well as the data analysis techniques were chosen based on the type of research problem.

2.2.1.4. Participants: people who were directly and indirectly involved

In conducting the research, the academic supervisors of this study were significantly involved in providing guidance on the research process. Furthermore, a number of IT security professionals within South Africa were involved as the research population for data collection.

2.2.1.5. Paradigm: shared way of thinking

Myers (2004) and Oates (2006) highlight three research paradigms to be considered when conducting research in information systems, namely, positivism, interpretivism, and critical research. The positivism paradigm assumes that reality is objectively given and can be described by measurable and scientific properties which are independent of the observer (researcher) and his or her instruments (Oates, 2006). Interpretivism is concerned with understanding the social context influences with the assumption that access to reality is only through social constructions such as language, consciousness and shared meanings (Myers, 2004).

Critical research is concerned with power relations, conflicts and contradictions with the assumption that social reality is historically constituted and that it is produced and reproduced by people (Myers, 2004). Table 2.1 presents the characteristics of the three research paradigms.

Table 2.1 The Research Paradigms

Positivism	Interpretivism	Critical research
Validity	Trustworthiness	Emancipation
Objectivity	Confirmability	Critique of tradition
Reliability	Dependability	Non-performative intent
Internal validity	Credibility	Critique of technological determinism
External validity	Transferability	Reflexibility

Source: Oates (2006)

Existing literature reveals that the positivist and interpretive paradigms are the two main paradigms mostly used within the field of information systems (Oates, 2006). Based on the research problem being investigated in this study, the positivism research paradigm has been identified as the most suitable philosophical assumption. This is based on the fact that the research objective, the research strategy, and the data gathering processes are strongly associated with the positivism research paradigm (Rajasekar, et al., 2013). The characteristics of positivism, presented in Table 2.1, align with the characteristics of this study. This is because this study uses foundational theories which are derived from valid and objective global best practice frameworks and standards to formulate the proposed ITSRB approach.

2.2.1.6. Presentation: means through which the research is disseminated and explained to others

This study is conducted in order to fulfil the requirements of a specific academic degree. The product of this study is a dissertation. The dissertation produced will be available and shared with the academic public as well as professionals in the field of IT security. Furthermore, opportunities to present this study in academic conferences will be used to ensure that the proposed ITSRB approach is used as widely as possible.

Figure 2.2 presents the research methodology that was executed for this study. It also shows the theory formulation process, chosen research strategy, chosen data generation, and chosen data analysis techniques highlighted in red.

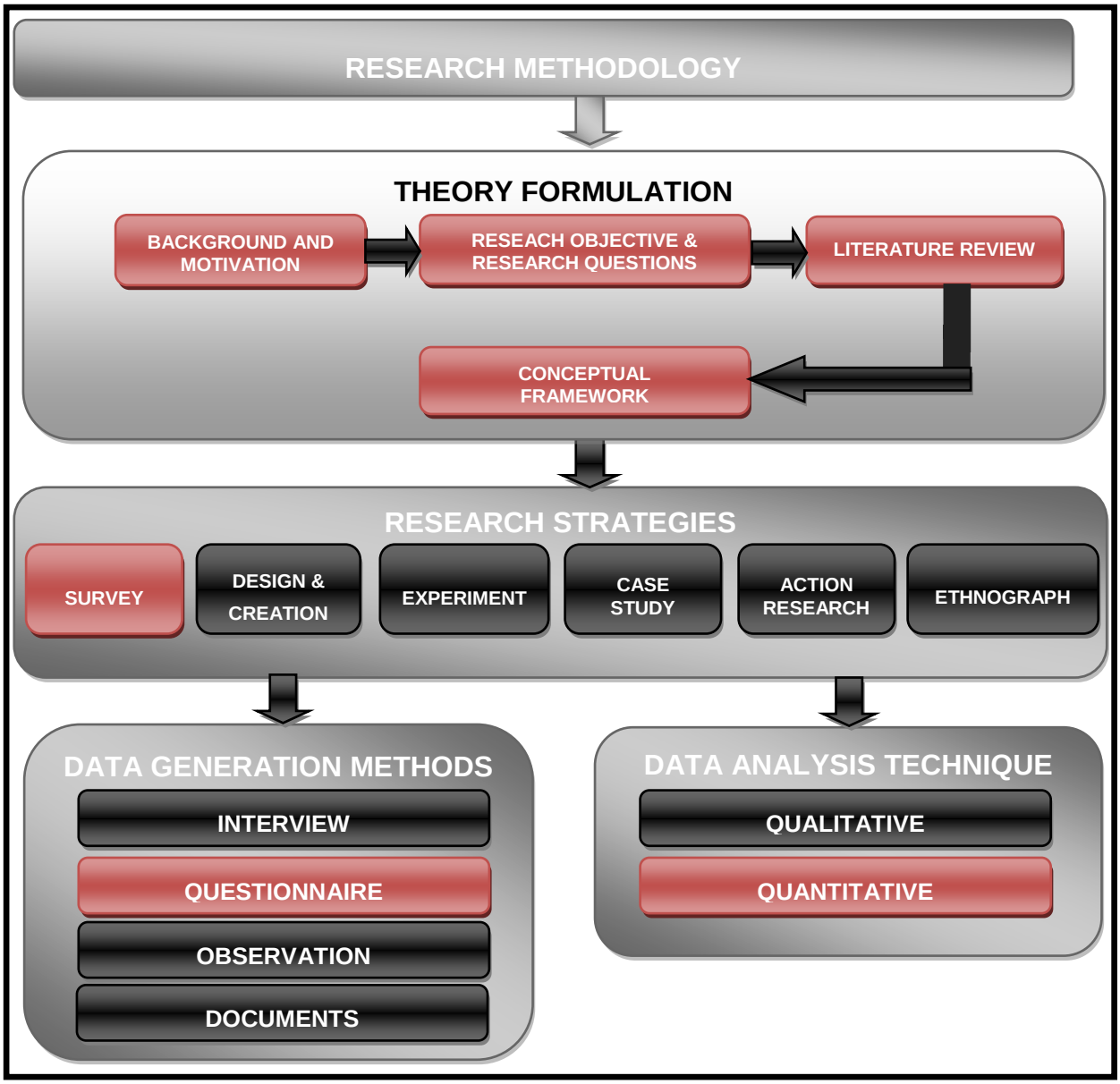

Figure 2.2 The Research Methodology Model

Source: Oates (2006)

The sections that follow describe the research methodology used in this study.

2.2.2. Theory formulation

In formulating the theory for this study, a literature review was conducted to uncover existing gaps within the field of IT security. The analysis revealed that there were common trends of poor risk management practices within the field of IT security, also recommended as a point for future research (Krichene, 2008). From the literature

review, the motivating factors were discovered, and the research objective and sub-objectives were formulated.

2.2.2.1. Background and motivation

This study was motivated by the following factors observed during the preliminary literature review:

- ***Increasing trend of IT security attacks*:** Despite the efforts that organisations employ to reduce IT security risks, the trend of IT security attacks is still increasing (Krichene, 2008; Netland, 2008; Straub, 2011). Failure to ensure that IT security risk is mitigated adequately may have dire consequences, resulting in reputational damage and financial losses.

- ***Poor risk management practices*:** Often superseding the technological risk aspects of IT security, many organisations leave the responsibility of managing IT security risk to IT security technologists because of the complexity of this discipline (Soo Hoo, 2000). Rather than treating IT security as just an independent technical concern, it should be considered as another risk that needs to be managed alongside all other business risks by professional risk managers (Soo Hoo, 2000; Foley, 2009). IT security is not just about technology; it is about the business (Van Cleeff, 2010).

- ***The incomplete mitigation of IT security risk*:** Organisations employ security technologies such as firewalls, intrusion detection systems (IDS), encryption, biometric systems, and other authentication systems to protect themselves against IT security attacks (Ogut, 2006). However, complete prevention of IT security breaches is technologically impossible and prohibitively expensive (Klemen & Biffl, 2004; Reid & Gilbert, 2007). For these reasons, organisations struggle to determine what controls to prioritise in mitigating IT security risk (Reid & Gilbert, 2007).

2.2.2.2. Research objectives

The main objective and sub-objectives that guided this study are revisited below.

2.2.2.2.1. Main objective

The main objective of this study is to investigate whether strong characteristics of the existing IT security frameworks and standards, the basic risk management principles, and the IT security threat modelling processes within the best practice body of knowledge can be extended to develop a formal and proactive approach for managing IT security risk.

2.2.2.2.2. Sub-objectives

The sub-objectives of the study are as follows:

1. *Investigate the best practice IT security frameworks and standards which are most commonly used within the financial institutions in South Africa by identifying their common characteristics and limitations.*
2. *Investigate basic risk management principles and IT security threat modelling processes to assess their benefits for IT security risk management.*
3. *Consolidate the strong characteristics of the investigated IT security frameworks and standards, basic risk management principles, as well as IT security threat modelling processes to develop characteristics and attributes of a dynamic IT security risk management approach.*

Having discussed the theory formulation of this study, including the research paradigm, the background and motivation as well as the objectives of this study, it is important to discuss the research strategy that is used. The following section discusses the research strategy executed.

2.2.3. Research strategy

A research strategy refers to the overall approach used to achieve the research objective and answer the research question (Oates, 2006). Oates (2006) and Sivasubramaniyan)2012(describe six strategies which can be used to conduct research in the field of information systems, namely, survey; design and creation; experiment; case study; action research; and ethnography.

2.2.3.1. Examples of research strategies

This section discusses the research strategies used in the field of information systems.

2.2.3.1.1. Survey

According to Kalain (2008), a survey is a systematic research strategy for gathering data from an illustrative sample of individuals using instruments composed of closed-ended and/or open-ended questions, observations or interviews.

2.2.3.1.2. Design and creation

Design and creation focus on developing new IT artifacts or products (Oates, 2006). The development of new IT artefacts involves creating new knowledge that demonstrates academic qualities with emphasis on improvement and invention (Kalain, 2008).

2.2.3.1.3. Experiment

Experiment refers to the process investigating cause-and-effect relationships, through testing of hypotheses to prove or disprove causal links between a factor and an observed outcome (Sivasubramaniyan, 2012).

2.2.3.1.4. Case study

A case study focuses on one instance that is to be investigated in order to gain detailed insight of that single instance (Oates, 2006). A case study is preferred in examining contemporary context when the relevant behaviours cannot be manipulated (Kalain, 2008).

2.2.3.1.5. Action research

Action research focuses on conducting research in the real world and then reflecting on what happened (Oates, 2006). Action research is a practical approach to researching either to solve an immediate problem or to gain insight through a reflective process of progressive problem-solving (Sivasubramaniyan, 2012).

2.2.3.1.6. Ethnography

Ethnography is described as the study of cultures through close observation and interpretation (Kalain, 2008). Ethnography focuses on getting a detailed understanding of a specific culture through participating in the field (Oates, 2006).

2.2.3.2. Conceptual framework used in this study

To test the conceptual framework (i.e. the ITSRB approach) proposed in this study, a survey was selected as a research strategy. A survey was chosen because it was most suitable for assessing the level of agreement on the characteristics of the ITSRB approach from the research sample in a systematic way. Furthermore, Adèr, Mellenbergh, & Hand (2008) highlight that surveys are one of the widely used research strategies that can be used to look for patterns in large groups of people for generalising responses.

Surveys are not limiting because they allow the researchers to use a variety of data generation methods as well as a variety of delivery methods including questionnaires, interviews, observations and documents (Dawson, 2002). According to Oates (2006), surveys are strongly associated with the positivism paradigm, as they seek patterns and generalisations.

There are a number of drawbacks to using surveys, including lack of depth; low response rates; inability to establish cause-and-effect relationships; and poor levels of accuracy (Adèr, et al., 2008). However, every research strategy has its own drawbacks, and in this case, the benefits of using a survey outweighed the disadvantages thereof.

The planning for conducting the survey for this study was structured according to six activities, as recommended by various authors (Dawson, 2002; Oates, 2006; Adèr, et al., 2008). These activities include data requirements, data generation method, data analysis technique, measurement, measuring scale and validity testing.

2.2.3.3. Data requirements

To conduct a survey, the researcher needs to consider the type of data that needs to be generated (Oates, 2006). Since this study intends to assess the characteristics of the ITSRB approach as well as its applicability effectiveness, the survey ensured that the data gathered from the sample size is directly associated with the research objective and research question. Additionally, the survey was structured in a way that allows for a seamless analysis of data patterns and interpretations.

2.2.3.4. Data generation method

A data generation method is described as a means by which a researcher will produce data (Kalain, 2008). Oates (2006) outlines four types of data generation methods, namely, interviews, questionnaires, observations, and documents. An interview refers to a controlled conversation between the researcher and the respondent, where the researcher asks questions associated with the research topic being investigated (Sivasubramaniyan, 2012).

A questionnaire refers to research conducted through the use of a predefined set of questions, assembled in a predetermined manner (Trobia, 2008). Observation refers to the process of a researcher watching and paying attention to what people actually do instead of what they report they do (Oates, 2006). Documents data generation method refers to the process of using existing documents to investigate a specific research topic (Oates, 2006).

According to Trobia (2008), the most commonly used technique for collecting data for a survey is a questionnaire. After careful examination of the available data generation methods which could be used to collect data for this study, a questionnaire was identified as the preferred data generation method. A questionnaire was selected because of its ability to allow for predefined questions relating to the ITSRB approach.

Existing literature demonstrates that the Internet offers researchers the possibility of accessing many people quickly and cheaply (Fricker & Schonlau, 2002; Trobia, 2008). In delivering the questionnaire for a survey, an email or a website can be

used (Oates, 2006). Fricker and Schonlau (2002) conducted a study to assess the key characteristics of using Internet surveys (i.e. response rate, timelines, data quality and cost) and the results illustrated that Internet-based surveys offer more advantages over conventional surveys, depending on the target population.

This is because Internet surveys are easier to create and can be delivered quicker, at the click of a button (Fricker & Schonlau, 2002; Oates, 2006). The main challenges are associated with accuracy of data as well as the potential low response rate that can be controlled when the researcher creates the survey via input data validation processes and larger sample groups respectively (Fricker & Schonlau, 2002).

A number of authors (Cobanoglu, et al., 2001; Eaton & Struthers, 2002; Perkins, 2004) have demonstrated the many benefits that can be realised from using Internet-based surveys, some of which are summarised as follows:

- **Cost efficient:** Internet-based surveys are less expensive than traditional paper-and-pencil, physical mail, fax and telephonic survey methods. Fewer material resources of paper, ink, and mailing are required.

- **Broader sample size:** The potential pool of participants that can be reached via Internet-based surveys is much larger than other traditional methods.

- **High availability:** Internet-based surveys are available all the time at a location that is convenient for participants.

- **Fast delivery and response rate:** Internet-based surveys allow for shorter delivery time to participants. The response rate is higher, as there is less effort required from the participants.

- **More flexible:** Internet-based surveys allow the researcher to use various interactive and dynamic instruments such as images, videos, text and audio transmission.

- **Improved data quality:** With Internet-based surveys, the researcher is able to control the responses by putting in place input validation processes (e.g. a text field which only allows numbers). In some instances, there is even no need for manual data entry. Easier analysis, direct transmitting (i.e. through coding and analysis) of data is more accurate and there are more complete responses to open-ended questions.

On the contrary, there are other researchers (Sheehan, 2001; Fricker & Schonlau, 2002) who have revealed some of the key disadvantages of Internet-based surveys, which include the following:

- **Lower response rates:** No commitment from participants because there is no reward or motivation for participating.

- **Higher resistance:** Participants may often mistake such surveys as spam email with the threat of viruses.

In order to mitigate the potential risk of non-response, all the participants of the survey were contacted and provided with a formal invitation letter (Appendix A) before the survey was sent out (found in Appendix A). The formal invitation letter specified the title of the study, the objective of the study, the objective of the survey, and the survey process and timelines. Upon completion of the survey, the results are shared with the respondents.

Furthermore, an application for ethical clearance had to be made to the university (i.e. University of South Africa (UNISA)) to ensure that the questionnaire that is sent for the purposes of this study satisfies the minimum requirements and principles set by UNISA. The ethical clearance letter is presented in Appendix B.

This study collected data through the use of an Internet-based questionnaire. The questionnaire used in conducting the survey was developed in a manner that allowed for respondents to assess the attributes and elements of the proposed ITSRB approach in order to ascertain its effectiveness. Additionally, the Internet-

based questionnaire was selected because of its ease of use and creation, quick delivery, and easy accessibility.

2.2.3.5. Data analysis technique

Some authors (Fricker & Schonlau, 2002; Oates, 2006; Rajasekar, et al., 2013) state that the two main data analysis techniques for conducting research are quantitative and qualitative techniques. Quantitative data analysis is based on the measurement of quantity or amount where the results are essentially a number or a set of numbers (Oates, 2006). Qualitative research is concerned with quality and non-numeric data (Fricker & Schonlau, 2002; Oates, 2006). Qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and description of things (Berg, 2004). Table 2.2 contrasts the characteristics of the two data analysis techniques (Rajasekar, et al., 2013).

Table 2.2 – Data Analysis Techniques

Quantitative	Qualitative
Numerical, non-descriptive, applies statistics or mathematics and uses numbers.	Non-numerical, descriptive, applies reasoning and uses words.
Iterative process whereby evidence is evaluated.	It aims to get the meaning, feeling and description of the situation.
The results are often presented in tables and graphs.	Qualitative data cannot be graphed.
It is conclusive.	It is exploratory.
It investigates the what, where and when of decision-making.	It investigates the why and how of decision-making.

Source: Rajasekar, et al. (2013)

The quantitative data analysis technique was selected for this study, as it possesses characteristics that are suitable when attempting to make generalisations and seeking data patterns for a survey research. According to Oates (2006), the quantitative data analysis is the main type used in surveys and experiments.

2.2.3.6. Measurement

In order for survey research results to be assessed, there should be some form of measurement criteria that are applied on the results (Dykema, et al., 2008). Measurement is described as the process of associating values to characteristics of individual aspects to indicate their position in relation to the fundamental concept (Dykema, et al., 2008).

There are five levels of measurements as defined by Oates (2006) and Gershkoff (2008), namely, nominal, binary, ordinal, interval, and ratio. The numeric values of the variables follow an increasing trend as the ranges move from nominal level to ratio level (Dykema, et al., 2008; Gershkoff, 2008). These levels of measurement are described below.

Nominal measurement: With nominal measurement level, there is no relationship between the numeric values of the specified variable and characteristics that those variables represent (Oates, 2006; Gershkoff, 2008). For researchers to use nominal variables for association, they must first be parted into sequences of binary values (Gershkoff, 2008). Statistical calculations (e.g. average, median and variance) as well as computations such as correlations and regressions cannot be performed on nominal data because they will have no native meaning (Gershkoff, 2008).

Binary measurement: Oates (2008) defines binary variables as special nominal variables that can have two mutually exclusive values. Unlike nominal variables, binary variables can be used in association analyses (Gershkoff, 2008). For example, a variable can be given to gender (i.e. 0 = male and 1 = female) in a questionnaire. Under normal circumstances, there is no way that someone can be both male and female at the same time (i.e. they can be either male or female). Furthermore, there is no mathematical relationship between the number zero being male and the number one being female.

Ordinal measurement: Ordinal variables are variables that have assigned values which can be ranked or methodically categorised (Gershkoff, 2008). According to Gershkoff (2008), general comparison analyses can be performed between ordinal variables; however, it is not possible to make mathematical comparisons between

the values of the variable. For instance, a researcher might ask the participants' views about a certain subject (e.g. 5 = very high, 4 = high, 3 = medium, 2 = low, and 1 = very low). In this instance, it is possible to rank the values as well as make general comparisons between the values (e.g. 5 = very high is greater than 4 = high), but one cannot assume that a response of four is twice the value of the response of two (Gershkoff, 2008).

Interval measurement: Interval variables are variables where distances between the values of the variable are equal and mathematically meaningful, but the assignment of the zero value is illogical (Gershkoff, 2008). With interval variables, researchers are able to use a full range of parametric statistics because the differences between values allocated to the variables are meaningful (Gershkoff, 2008).

Ratio measurement: Ratio variables can be defined as variables where distances between values allocated to the variables are mathematically meaningful, and zero is a logical value (Gershkoff, 2008). With ratio variables, it is possible to analyse parametric associations and various mathematical computations such as addition, subtraction, multiplication and division, and such computations can be performed on the assigned values (Gershkoff, 2008). Likewise, it is possible for statistical computations such as the mean, median, mode and variance to be performed (Gershkoff, 2008).

This study uses the ordinal measurement level for measuring the survey responses from the research sample. The ordinal measurement offers more meaningful results than nominal and binary measurements even though it is less statistically powerful than interval and ratio measures (Dykema, et al., 2008).

Since the intention of the survey used in this study was to get the participants' views on the ITSRB approach and test if the approach would actually add more value on how they manage IT security risk, variables across a range will be measured. As previously stated, ordinal measures can be used to demonstrate information about the relationship between two values (e.g. 5 = very good and 4 = good), indicating that one value is greater than the other (Gershkoff, 2008; Dykema, et al., 2008).

Moreover, ordinal measures are logically obtained with ordinal scales which normally use close-ended questions and answers where categories are classified either using numbers only, words only or a combination of both (e.g. a Likert scale which include classification of both positive and negative results) (Dykema, et al., 2008). A typical example is where research participants are probed to provide their level of agreement with a certain statement, with response options as follows: 5 = strongly agree; 4 = somewhat agree; 3 = neither agree nor disagree; 2 = somewhat disagree; and 1 = strongly disagree. For this reason, the characteristics that ordinal measures possess substantiate the motives for using them for the survey in this study. This way, the data quality will be optimised; the measures being used will be more reliable and valid; and the quantitative analysis will be more feasible.

2.2.3.7. Measuring scale

The choice of a measuring scale when a questionnaire is designed is very important (Brill, 2008). An ordinal scale was used for this study, as it seemed to be the most appropriate measuring scale. The Likert scale is one of the common forms of ordinal measuring scales and will be used for the questionnaire (Brill, 2008). Brill (2008) describes the Likert scale as a special type of the more general class of summated rating scales created from multiple ordered-category rating items. It has the following distinctive characteristics, as defined by Brill (2008):

- Each item uses a set of proportionally balanced bipolar response categories which indicate varying levels of agreement or disagreement with a specific statement expressing an attitude or opinion.
- The response category points for each item are individually labelled (e.g. strongly agree, agree, disagree, strongly disagree) and typically include four or more points.
- The descriptive text of the chosen labels should demonstrate similar progressions or gradations between each pair of consecutive points.

A Likert scale which has five categories has been selected for this study, with the points defined in Table 2.3.

Table 2.3 – The Likert Scale (used in this study)

Scale Value	Scale Description
1	**Strongly Disagree:** Indicates that the respondent **certainly does not** agree with the statement presented.
2	**Disagree:** Indicates that the respondent **probably does not** agree with the statement presented.
3	**Neither Agree nor Disagree:** Indicates that the respondent does not have a viewpoint about the statement presented.
4	**Agree:** Indicates that the respondent **does** agree with the statement presented to some level.
5	**Strongly Agree:** Indicates that the respondent **certainly does** agree with the statement presented.

The scale descriptions were modified in each section of the questionnaire to assess the respondents' level of agreement with that presented statement. This type of Likert scale was selected because it seemed more viable to analyse the values of the score after the data collection process.

2.2.3.8. Validity testing

To determine the effectiveness of the survey for this study, it was deemed necessary to pretest it before using it (Chisnall, 1997; Hutt & Speh, 2001; Singh, 2007). Pretesting assists in assessing the reliability, validity, accuracy, integrity and ambiguity of the questionnaire. It also assists in identifying any omission of important factors and assists in examining any requirements to integrate or remove certain factors from the questionnaire (Chisnall, 1997; Hutt & Speh, 2001).

Furthermore, pretesting a survey usually involves validity testing. It will assist in identifying weaknesses such as question format, order of questioning, as well as reduce the risk of obtaining incorrect answers (Chisnall, 1997).

Validity is primarily a measurement term which refers to the relevance of a measuring instrument for a particular objective (Knapp, 2008). Validity is concerned about whether findings are actually about what they appear to be about (Chisnall, 1997; Knapp, 2008).

There are two types of validity which should be evaluated in quantitative research: internal and external validity (Singh, 2007). Internal validity is the consistency with which the study is conducted (e.g. the manner in which measurements were taken), whereas external validity refers to the extent to which the research results would be generalised to other circumstances (Howell, et al., 2005). In simple terms, research conducted is considered to have external validity if the results can be generalised (Howell, et al., 2005).

There are several types of validity which are explained within various pieces of literature:

- **Content validity:** This is the extent to which a measurement reflects the specific intended domain of content (Howell, et al., 2005).

- **Face validity:** This refers to how a measure or a procedure appears and is normally required when a new measure is developed (Bryman & Cramer, 2001; Howell, et al., 2005). Face validity intuitively assesses the measure by asking other people if the measure seems to capture the concept or not (Singh, 2007).

- **Construct validity:** It refers to the process of seeking agreement between a specific measurement tool or procedure and a theoretical concept (Howell, et al., 2005).

- **Criterion-related validity:** It is used to reveal the accuracy of a measure or procedure by comparing it with another measure or procedure that has been demonstrated to be valid (Bryman & Cramer, 2001). Criterion-related validity is also referred to as instrumental validity (Howell, et al., 2005).

After much consideration, content validity is the most appropriate validity type for this study. This is due to the fact that the proposed questionnaire attempts to measure opinions and attitudes of individuals from the target population towards the ITSRB

approach proposed in this study with the objective of evaluating internal and external validity.

2.3. DATA COLLECTION

The preceding sections described the research methodology followed in conducting this study. This section presents the data collection process followed. The behaviours, thoughts and attitudes of IT security professionals are assessed to determine their level of agreement with the attributes and characteristics of the ITSRB approach. A survey was selected as a research strategy using a questionnaire as a data generation method. A set of closed-ended questions were used in order to collect individual data about one or more specific topics relating to the characteristics of the ITSRB approach.

2.3.1. Research Objective Mapping

The main objective of this study is to investigate whether strong characteristics of the existing IT security frameworks and standards, the basic risk management principles, as well as the IT security threat modelling processes within the best practice body of knowledge can be extended to develop a formal and proactive approach to managing IT security risk. There were three sub-objectives defined in order to achieve the main research objective. The questionnaire (Appendix C) was developed in a way that ensured alignment to the research objective, thereby linking each section to the sub-objectives. Figure 2.2 presents the mapping of the questionnaire to the research sub-objectives and research questions.

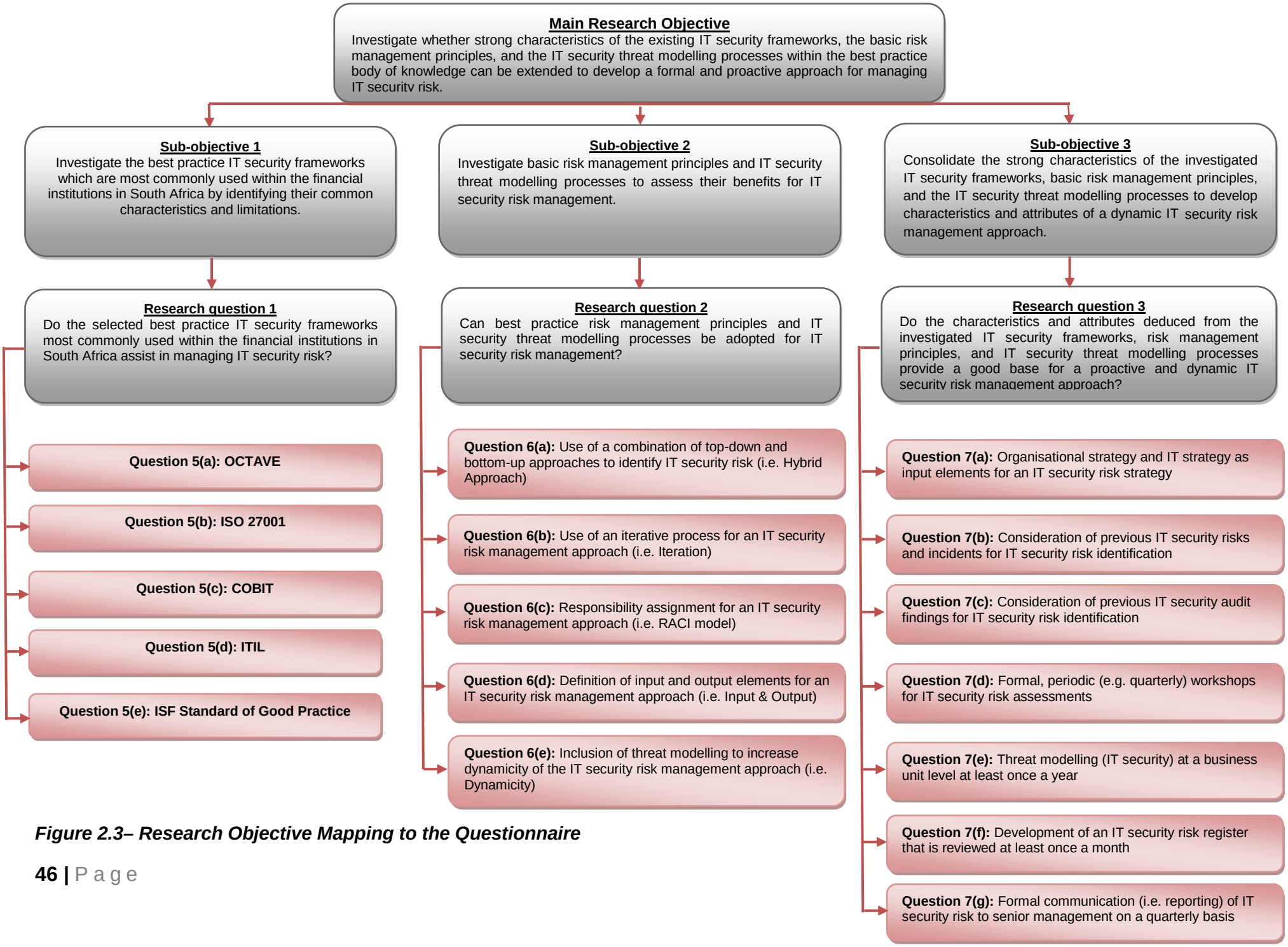

Figure 2.3– Research Objective Mapping to the Questionnaire

The full questionnaire of the survey is found in Appendix C. Section 1 of the questionnaire aimed to gather information about the demographics of the respondents with the objective of determining if they actually fall within the target population. Section 2 of the questionnaire is aligned to the first research sub-objective. The objective of section 2 is to evaluate the respondents' views about the selected frameworks and standards' ability to manage IT security risk.

Section 3 of the questionnaire evaluates the attributes of the proposed approach. The attributes were extracted from the best practice IT security frameworks and standards, risk management principles, and threat modelling. Section 3 of the questionnaire is aligned to the second research sub-objective.

Section 4 of the questionnaire is aligned to the third research sub-objective. Section 4 of the questionnaire assesses the core characteristics of the proposed ITSRB approach in order to evaluate the respondents' level of agreement on its ability to assist in managing IT security risk.

2.3.2. The Questionnaire

The questionnaire was created by means of SurveyMonkey, a web-based survey tool. The questionnaire was structured into five main sections, namely, the introduction; the background about the respondent and their professional experience; best practice risk management frameworks and standards for IT security; approach to IT security; and the primary principles of the proposed ITSRB approach.

Questionnaire design

In designing the questionnaire, the following principles proposed by Barribeau, et al. (2005) were followed:

- **Directness:** This principle ensures that questions are specifically tailored for a group of respondents, and are written in a straightforward and direct language.
- **Simplicity:** This principle ensures that questions are kept short, simple and do not have complex information which has to be learned before respondents answer questions.

- **Specificity:** This principle ensures that more specific questions are asked as opposed to general ones.
- **Discreteness:** This principle ensures that questions that are overly personal are avoided (e.g. in cases when dealing with sensitive issues).

To encourage researchers to format questions in a consistent manner, Barribeau, et al. (2005) proposed that the following types of questions should be avoided:

- double-barreled questions which compel respondents to make two decisions in one;
- double negative questions which can lead to ambiguous answers;
- hypothetical questions which typically require more scrutiny;
- biased questions which indicate the researcher's feelings or attitudes towards a topic; and
- questions with long lists which may exhaust respondents' trail of thinking.

To avoid ambiguity when designing the questionnaire, the principles recommended by Barribeau, et al. (2005) were applied. Further, Trobia (2008) states that questionnaires should usually be composed of three main parts: the introduction (or cover letter) including the instructions, the main body, and a 'thank you note' to the respondents for their contribution.

The cover letter is one of the key elements of improving the response rate because it introduces the research, explains the aim of the research and attempts to motivate the respondents to cooperate with the survey objectives (Trobia, 2008). Additionally, Trobia (2008) highlights that the cover letter should guarantee the confidentiality and anonymity of the respondents.

The questionnaire for this study follows the structure that is proposed by Trobia (2008), and the questions were designed according to the principles stated by Barribeau, et al. (2005). The questionnaire started off with the introduction (or cover letter) which

specifies the objective of the survey as well as provides instructions to the respondents. Instructions are imperative especially in self-administered questionnaires because they provide the respondents with all the rules that must be followed in answering the questions (Trobia, 2008).

The introduction provided information about the background of this study and why it is being conducted. The first section primarily collected information about the background of each respondent with the objective of discovering their level of experience within the field of IT security as well as the size of the organisation that they work for. The first section provided three options for the respondents to choose from.

The main body of the questionnaire was made up of three sub-sections which have close-ended questions (i.e. section 2 to section 4). The questions in these sections utilised a 5-point Likert scale that provided categories of both positive and negative values to indicate the level of agreement of the respondent for each statement presented. The response options ranged from “strongly disagree”, “disagree”, “neither agree nor disagree”, “agree” to “strongly agree”.

The second section presented the IT security frameworks and standards which were used as a basis for the proposed ITSRB approach. The idea behind this section was to determine how much the respondents agree with the frameworks and standards’ ability to manage IT security risk.

The third section assessed the attributes of the proposed ITSRB approach to test the respondents’ level of agreement with its basic attributes. The fourth section was used to test the respondents’ level of agreement with the characteristics of the proposed approach. Lastly, the questionnaire ended with a conclusion which thanked the respondents for participating in the survey.

2.3.3. Population size

Population size refers to the total number of people that are eligible to participate in a survey (Penwarden, 2014). To determine the population size of IT security professionals within the financial institutions of South Africa, data from the Private Security Industry Regulatory Authority (PSiRA) was used. PSiRA is a regulatory

authority in South Africa responsible for regulating both the private and public security industry to ensure the public and national interest of the security industry. It is important to note that all financial services institutions listed on the South African stock exchange are regulated by PSiRA (PSiRA, 2014).

For this reason, the population size for security professionals within South African financial institutions will be less than the population size specified by PSiRA because PSiRA's data encompasses other security professionals outside financial institutions. Analysis revealed that the population size of IT security professionals within South Africa was 476 in 2014 (PSiRA, 2014). To ensure that an adequate confidence level and margin of error are achieved for this study, a population size of 500 was assumed.

Penwarden (2014) emphasises the importance of considering the size of the target population, the sample size, the confidence level, as well as the margin of error to avoid guessing. Table 2.41 presents the effects of these parameters (i.e. population size, sample size, confidence level, and error margin) on the accuracy of the results.

Table 2.4– Level of Accuracy Parameters

Parameter Name	Value Increased	Value Decreased
Population Size	Accuracy Decreases	Accuracy Increases
Sample Size	Accuracy Increases	Accuracy Decreases
Confidence Level	Accuracy Increases	Accuracy Decreases
Margin of Error	Accuracy Decreases	Accuracy Increases

Source: Penwarden (2014)

Sample size refers to the number of people that are selected to participate in a survey (Penwarden, 2014). A higher sample size provides a higher confidence level. The confidence level describes how certain a researcher can be that their results are correct, with a value of between 90% and 99% being acceptable for surveying (Penwarden, 2014). A higher confidence level increases the accuracy level of the results (Penwarden, 2014). The margin of error refers to the potential amount of random sampling error in a survey's results (Penwarden, 2014). A higher error margin decreases the level of accuracy in the results (Penwarden, 2014).

In calculating the sample size for this study, the parameters recommended by Penwarden (2014) were considered (i.e. population size, sample size, confidence level, and margin of error). The population size was approximately 500 individuals, based on the data sourced from PSiRA (2014). Penwarden (2014) stated that an average response rate for an email survey that has a link to a web-based survey is about 24.8%. Acknowledging that the response rates for web-based surveys are very low, a confidence level of 90% and a margin of error equal to 10% were used to determine the minimum sample size of 60.

The questionnaire was sent to 150 IT security professionals within South African financial institutions. The target was to get at least 60 responses in order to achieve an acceptable confidence level of 90%. The questionnaire consisted of 21 questions which were dispersed amongst the four sections illustrated in Figure 6.2 found in section 6.2 of this chapter.

2.3.4. Target population

The target population is the total group of individuals from which the sample is drawn (Penwarden, 2014). The target population consisted of individuals who work for different financial institutions within South Africa including Standard Bank, Absa, Nedbank, FirstRand, Alexandra Forbes, Mutual & Federal, Momentum, and Old Mutual. The questionnaire was administered to personnel who are directly or indirectly involved with IT security risk management, IT security governance, IT security operations, and IT security advisory. The roles of the sample group included IT security officers; IT security managers; IT security internal and external auditors; IT security operations personnel; IT risk managers; and IT security risk consultants.

The questionnaire's invitation letter was sent to the indicated sample group via email with the link to the questionnaire included. The initial communication detailed the purpose of the study, process and timeline. The questionnaire's invitation letter is in Appendix A.

Confidentiality of the responses was ensured because the questionnaire was designed in a way that made it impossible to determine who responded. Respondents' computer public IP addresses could be seen from SurveyMonkey; however, because most

organisations make use of dynamic IP addresses, it would be a challenge to trace any IP address back to a specific person (Van Horne, et al., 2001).

Dynamic IP addressing refers to a method for remotely connecting client computers to a communication network by way of a server system, thereby allowing client computers to change IP addresses with every connection (Miller, 2001; Van Horne, et al., 2001). It was therefore not possible to know who the different respondents were. This further strengthened the confidentiality and anonymity of the respondents.

2.3.5. Sampling

Oates (2006) states that there are two types of sampling techniques: probability and non-probability sampling. Probability sampling is used when there is a high probability that the sample of respondents chosen is a representation of the overall population being studied (Oates, 2006). With non-probability sampling, the research samples are gathered in a process that does not give all the individuals in the population equal chances of being selected (Oates, 2006). An overview of sampling techniques is depicted in Table 2.5.

Table 2.5 – Sampling Techniques

Probabilistic	Non-probabilistic
Random	Purposive
Systematic	Snowball
Stratified	Self-selection
Cluster	Convenience

Source: Oates (2006)

There are four types of probabilistic sampling, namely, random, systematic, stratified, and cluster probabilistic sampling (Oates, 2006). Random probabilistic sampling involves a random selection of the population being studied and is often carried out for widespread research (Oates, 2006). With systematic probabilistic sampling, the population must be listed in a random order based on the characteristics being studied. Systematic sampling is more precise than random sampling (Trochim, 2006). Stratified probabilistic sampling involves selecting a random proportion from random sampling, dividing the population into homogeneous sub-groups and then taking a simple random

sample in each sub-group (Oates, 2006). In cluster sampling, the population is divided into clusters; the clusters are randomly sampled and thereafter all the samples within the sampled clusters are measured (Trochim, 2006).

Similarly, there are four types of non-probabilistic sampling techniques; these are purposive, snowball, self-selection, and convenience non-probabilistic sampling techniques. In purposive sampling, the researcher samples with a purpose in mind and needs to reach a targeted sample (Oates, 2006). With snowball sampling, the researcher starts by identifying individuals who meet the criteria for inclusion in their study; thereafter, the researcher requests those individuals identified to recommend others whom they may know who also meet the criteria (Trochim, 2006). With the self-selection non-probabilistic sampling technique, the researcher publicises their need for samples, checking the relevant samples and thereafter inviting or rejecting the samples based on the specified criteria (Oates, 2006). With convenience non-probabilistic sampling, the researcher seeks volunteers to form part of their sample size and utilise them in the study assuming that they meet his or her criteria for the target population (Oates, 2006).

A non-probabilistic purposive sampling technique was used because its characteristics resonate with goals of conducting the survey for this study (i.e. to assess IT security professionals' level of agreement with the ITSRB approach). IT security professionals in the South African financial institutions were selected to participate in the survey, as they were more likely to produce valuable data that meets the purpose of this study.

To analyse the data collected, the quantitative data analysis technique was selected, as discussed in Chapter 2. The quantitative data analysis technique possesses characteristics that are suitable when attempting to make generalisations and seeking data patterns for a survey research such as this one. According to Oates (2006), quantitative data analysis is the main type used in surveys and experiments.

2.4. CONCLUSION

This chapter presented the research methodology used to conduct this study. Investigation of the literature revealed the survey strategy as the most suitable strategy for this study, as it possesses characteristics which are anticipated to assist this study in attaining the research objectives as well as answering the associated research questions.

Since there are different data generation methods which exist, an analysis was also conducted to review the advantages and disadvantages of the different methods available, and a questionnaire was selected as the most appropriate data generation method for this study. The delivery method selected was the Internet (i.e. web-based questionnaire), as it presented the most appealing characteristics that aligned to the objectives of this study. The quantitative data analysis technique was selected because it allowed for generalisations of data that would yield the findings of this study.

Furthermore, the data collection process followed as well as the questionnaire used for the survey were presented. The questionnaire was mapped to the research objective of the study to ensure alignment. The process of formulating the questionnaire was discussed. Furthermore, the process of administering the questionnaire including the population size, the target population and the survey tool used were presented.

The chapter that follows discusses the risk management and IT security frameworks and standards with the objective of understanding their benefits in managing IT security risk.

3. ANALYSIS OF FRAMEWORKS AND STANDARDS FOR IT SECURITY RISK

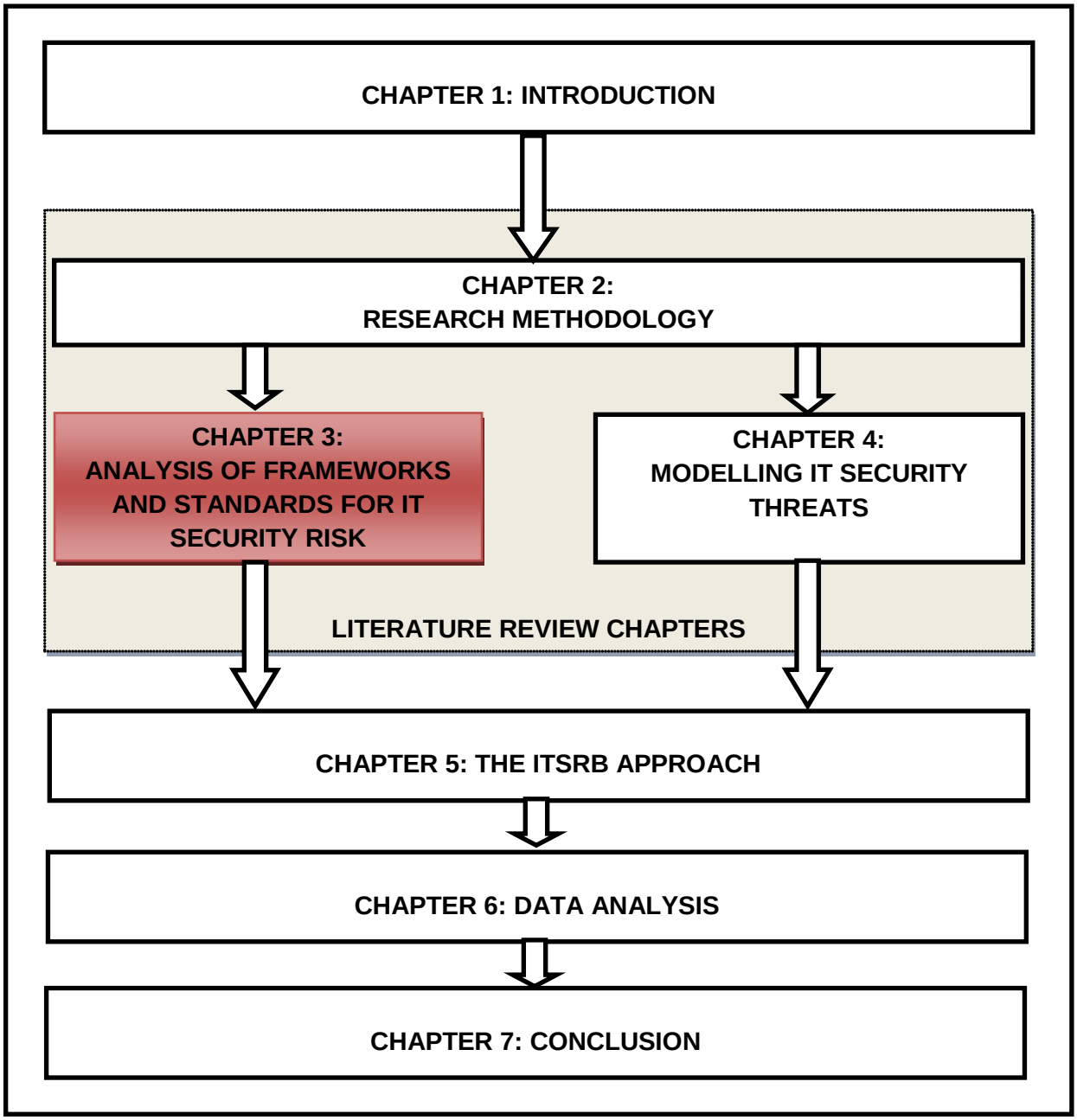

Figure 3.1 – Dissertation Layout: Chapter 3

3.1. INTRODUCTION

Management of IT security risk requires efficient and effective governance and risk management practices which are holistic, taking into account several interacting components (IT Governance Institute [ITGI], 2012). This chapter reviews the basic risk management frameworks as well as IT security frameworks and standards within the current body of knowledge. Since risk management forms an integral part of the proposed IT Security Risk Based (ITSRB) approach, it is discussed in depth in this chapter. Additionally, the basic concepts underlying the concept of IT security and the characteristics of the frameworks and standards are discussed in order to accentuate the importance of managing risk for IT security. The objective of reviewing characteristics of the frameworks and standards is to identify similarities which may exist amongst the frameworks and standards. The output of the review is leveraged when developing the ITSRB approach.

The foregoing chapter discussed the research methodology employed in this study. This third chapter is divided into five sections. Section 3.2 provides the background of the basic IT security concepts. Section 3.3 provides an overview of risk management for IT security. Section 3.4 presents the selected IT security frameworks and standards by analysing the strong areas and weaknesses of each framework and standard. The chapter concludes with Section 3.5.

3.2. BACKGROUND

Information is deemed to be a critical asset to any organisation regardless of the nature of the business because it enables business operations (Walser, et al., 2009). Today's world requires information to be accessible and dependable across the globe (Panda, 2009). Organisations use Information Technology (IT) to process their information for better support of their missions, business critical functions, as well as their strategies (Maphakela, 2008).

Furthermore, organisations and individuals always find themselves under pressure to stay abreast with current IT in order to run their businesses or their private lives better because of the need to communicate over the Internet (Krichene, 2008). Unfortunately,

this need for accessing the Internet also exposes organisations and individuals to a variety of threats that can have adverse effects on IT assets (Walser, et al., 2009).

The development of personal computers over the past 20 years is indicative of how change has been continuous in the field of IT (i.e. from big desktop computers to small mobile computing devices) (Winter & Schelp, 2008; Poolsappasit, 2010). The development of personal computers shows an increasing trend of personal portable devices which are Internet-enabled, allowing people to communicate in their own comfort (Winter & Schelp, 2008). The IT security threats emanating from desktop personal computers are different from the IT security threats emanating from portable personal computers (Poolsappasit, 2010). The changing environment in IT has therefore necessitated the need for IT security professionals to stay abreast with current technology to ensure that the correct IT security controls are put in place for the protection of IT assets (Winter & Schelp, 2008).

3.2.1. The need to protect IT assets

Today's world requires that digital data be accessible, dependable and protected from misuse (Panda, 2009). Information is deemed to be a critical asset to any organisation irrespective of the nature of the business (Walser, et al., 2009). In this digital era, organisations use IT to transform their information to better support their missions, business critical functions, and their strategies, which make IT one of the key enablers of business (Stoneburner, et al., 2002). The process of transforming information within the context of IT involves creating, processing, transmitting and storing of information with the use of IT (Whitman & Mattord, 2005). Information gathers meaning and value as it goes through the different processes of transformation (Panda, 2009). Information is a vital part of IT; as such, it is regarded as a significant IT asset (Whitman & Mattord, 2005; Panda, 2009).

Organisations have transitioned to conducting over 99% of their essential functions electronically using IT (Walser, et al., 2009). The motivation of this significant reliance on IT has shifted from egotistical to monetary, as the requirement for protecting IT has become a continuous point of concern (Walser, et al., 2009). Therefore, the need to protect IT assets has necessitated the discipline of IT security (Krichene, 2008).

3.2.2. The need for IT security

To safeguard IT, the process of IT security is applied. The goal of IT security is to protect the confidentiality, integrity, availability, non-repudiation and authentication of IT assets (Siponen & Oinas-Kukkonen, 2007). Confidentiality refers to the principle of preserving IT assets, thereby ensuring that information is not disclosed to unauthorised individuals, entities or processes (Taylor, et al., 2008).

Integrity is concerned with protecting unauthorised modification of IT assets, thus ensuring the completeness and accuracy of information (Bishop, 2005). Availability refers to the principle of ensuring that IT assets are accessible and usable upon demand by authorised entities (Bishop, 2005).

The goal of non-repudiation is to guarantee that parties involved in accessing IT assets cannot deny their activities at a later stage (Siponen & Oinas-Kukkonen, 2007). Authentication involves confirming the identity of people who access IT assets (Siponen & Oinas-Kukkonen, 2007).

Various pieces of literature use the terms “IT security”, “computer security”, “information security” and “information assurance” interchangeably, which all share the common goal of protecting the confidentiality, integrity and availability of information and IT (Ajibuwa, 2008). There are some subtle differences between the terms that define IT security, which lie primarily in the approach to the subject, the methodologies used and the areas of concentration (Taylor, et al., 2008; Ajibuwa, 2008). For the purpose of this study, the term “IT security” is used.

Having reviewed the basics of IT security, it is now important to examine the concepts of corporate governance and its sub-components. These include IT governance and risk management, which have been identified as an area of weakness within IT security (Krichene, 2008).

3.3. CORPORATE GOVERNANCE

Corporate governance is the framework that strategically monitors whether the outcomes of an organisation are in accordance with its set plans (Maphakela, 2008; Bradley & Pratt, 2011). Corporate governance involves many activities within an organisation which form an integrated system of administration, accountability and supervision (IT Service Management Forum [ITSMF], 2007; Tang-Jing & Shen-LePing, 2010; Bradley & Pratt, 2011). The goal of corporate governance is to ensure that leadership teams within organisations make their decisions in a responsible manner (ITSMF, 2007; Institute of Directors, 2009; PricewaterhouseCoopers [PwC], 2009). The two disciplines under corporate governance which form the basis of this study are IT governance and risk management.

Likewise, the King III Code, a global corporate governance framework, encourages organisations' boards to place great emphasis on ensuring that they are satisfied with the governance of IT and management of risk, as they form the cornerstones of corporate governance (Institute of Directors, 2009). For the purpose of this study, the principles recommended by King III Code (2009) have been adopted. These disciplines are discussed in the ensuing sections.

3.3.1. IT governance

The pervasiveness of IT has led to the development of a formal subset of corporate governance – IT governance (Institute of Directors, 2009; Bradley & Pratt, 2011). IT governance is described as a discipline that is primarily concerned with IT management processes, regulations, inspection standards, control frameworks and standards, measurement tools, and the protection of IT assets (Tang-Jing & Shen-LePing, 2010). IT governance enables the leadership of an organisation to adequately control the foundation and execution of IT through the existing organisational structures and processes to produce desirable results (Maphakela, 2008). IT governance assists organisations to better align their IT initiatives and the organisation's overall strategic objectives (Tang-Jing & Shen-LePing, 2010). The protection of IT assets necessitates a risk management process that aims to manage risk emanating from IT (Tang-Jing & Shen-LePing, 2010).

3.3.2. Risk management

To understand the intricacies that come with managing risk within IT security, it is important to understand the concept of risk management, as it provides the basis of how risk for IT security should be managed (Ketel, 2008). Risk management is described as the process of forecasting, evaluating and treating risks with the objective of minimising the impact of unacceptable risk (Felegyhazi, 2011).

The principal goal of an organisation's risk management process should be to protect the organisation and its ability to perform its mission, including its IT assets (Walser, et al., 2009). Risk management process within IT should not be treated primarily as a technical function carried out by IT experts who operate and manage the IT system but as an essential management function of the organisation alongside other business risks (Stoneburner, et al., 2002).

Risk management is an iterative process which should lead to continuous improvement in an organisation's risk posture (Ketel, 2008). Risk management is positioned as the cornerstone of corporate governance and greater emphasis is placed on the organisation's board to ensure that it is satisfied with the management of risk (Maphakela, 2008; Institute of Directors, 2009; PwC, 2009).

To achieve the goal of adopting a robust process for risk management, the ISO 31000 framework was adopted. ISO 31000 is a risk management framework developed by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), which are international bodies whose members are subject matter experts responsible for participating in developing international standards through technical committees (ISO/IEC 31001, 2009). ISO 31000 is cited as ISO/IEC 31000:2009 and provides principles, guidelines and a process for managing risk for any organisation regardless of its size, activity or sector (ISO/IEC 31001, 2009).

Figure 3.2 depicts the basic risk management framework based on ISO 31000. It highlights the key focus areas of a generic risk management process as well as the continuous life cycle of risk assessment, risk treatment, risk monitoring, and communication.

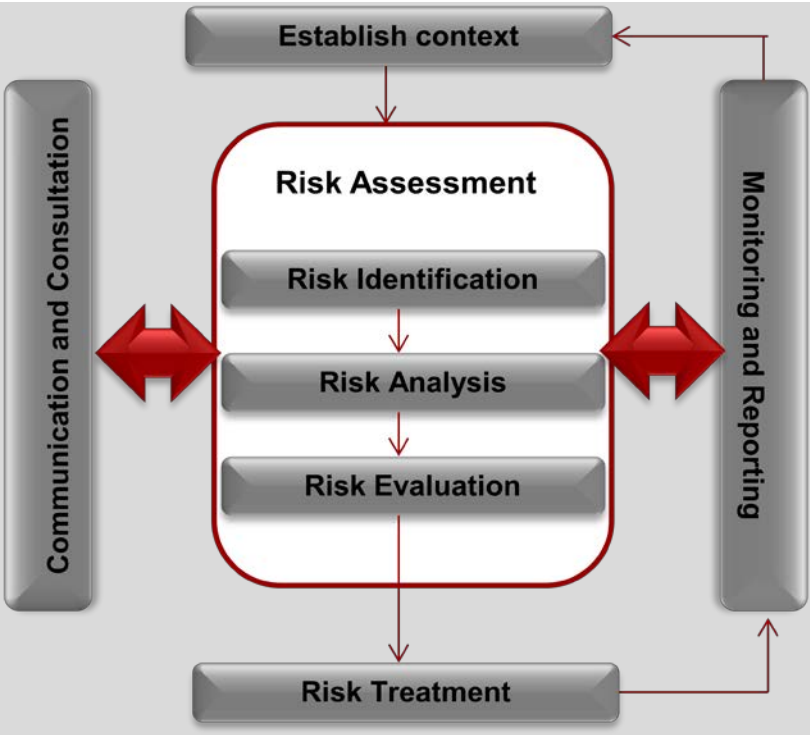

Figure 3.2 – Generic Risk Management Process

Source: ISO/IEC 31001 (2009)

3.3.2.1. Establish context

Prior to the commencement of a risk assessment process, a context setting activity must be carried out to determine the scope and boundaries of the assessment (ISO/IEC 31001, 2009). Establishing the context provides a basic understanding of the risk and its risk universe (Gibson, 2012). Furthermore, establishing the context assists in identifying the criteria that will be applied and the activities involved in determining the initial risk rating of the object being assessed (ISO/IEC 31001, 2009). The initial risk rating allows the risk assessment process to prioritise the assessments by focusing effort and resources on areas with higher risk (Ketel, 2008).

3.3.2.2. Risk assessment (risk identification, risk analysis and risk evaluation)

The risk assessment process consists of risk identification, risk analysis and risk evaluation. Risk identification establishes the exposure of the organisation to risk and uncertainty (Maphakela, 2008). This includes knowledge of the factors critical to success as well as the threats and opportunities related to the achievement of objectives (Gibson, 2012). The risk analysis and evaluation activity assists the effective

and efficient operation of the organisation by identifying risks that require attention from management (Commission, 2015). Moreover, the risk assessment activity provides organisations with the ability to prioritise risk and control actions with respect to their potential for benefiting the organisation (Institute of Risk Management [IRM], 2010).

3.3.2.3. Risk treatment

Risk treatment is the process of selecting and implementing measures to control risk (IRM, 2010). Risk treatment consists of four options, namely, risk mitigation, risk avoidance, risk transfer and risk acceptance (Jahankhani & Nkhoma, 2009).

Risk mitigation refers to the process of implementing controls to reduce either the likelihood or the impact of risks that are borne by the object (Ketel, 2008). Risk avoidance is the process of evading the risk in a case where the cost and likelihood of the risk are large and it is no longer feasible to continue operation in the area of activity that incurs the risk (IRM, 2010).

Risk transfer is concerned with sharing the cost of the risk through tools such as insurance, contracts and warranties or joint-venture agreements in cases where the risk is part of the business, but the cost is predictable (ISO/IEC 31001, 2009). Risk acceptance refers to a case where the risk is unlikely to materialise or its impact is so low that it warrants no further action (Gibson, 2012).

3.3.2.4. Monitoring and review

During the process of risk assessment, it is imperative to monitor and review risk performance to ensure that the risks facing the organisation are still valid as well as to ensure that the organisation learns from past experiences (ISO/IEC 31001, 2009; IRM, 2010).

3.3.2.5. Communication and consultation

Communication and consultation are also considered to be part of the supporting activity in managing risk (ISO/IEC 31001, 2009). The key stakeholders or risk owners

should be kept informed about risk performance to ensure that focus is placed on the risk that matters (Institute of Directors, 2009; IRM, 2010).

Jahankhani and Nkhoma (2009) demonstrated in their study that risk is seldom eliminated; it is merely mitigated or controlled. This is the same reason that a risk management process is an endless or iterative loop (Gibson, 2012). Once a risk is mitigated, it should be periodically reviewed, and controls should be tested for compliance at regular intervals (Maphakela, 2008; Jahankhani & Nkhoma, 2009; IRM, 2010).

The relationship between corporate governance, risk management and IT governance is fundamental for organisations to deliver on their strategies and missions (Tang-Jing & Shen-LePing, 2010). According to Krichene (2008), there is a need to extend the principles of risk management into the area of IT security. Management of risk in IT security is an essential process in IT governance as well as corporate governance and has motivated the need for IT security risk management (Tang-Jing & Shen-LePing, 2010).

3.3.3. IT security risk management

The interpretation of corporate governance, IT governance and risk management adopted from King III Code (2009) are summarised in Figure 3.3 with the objective of highlighting the foundation of IT security risk management.

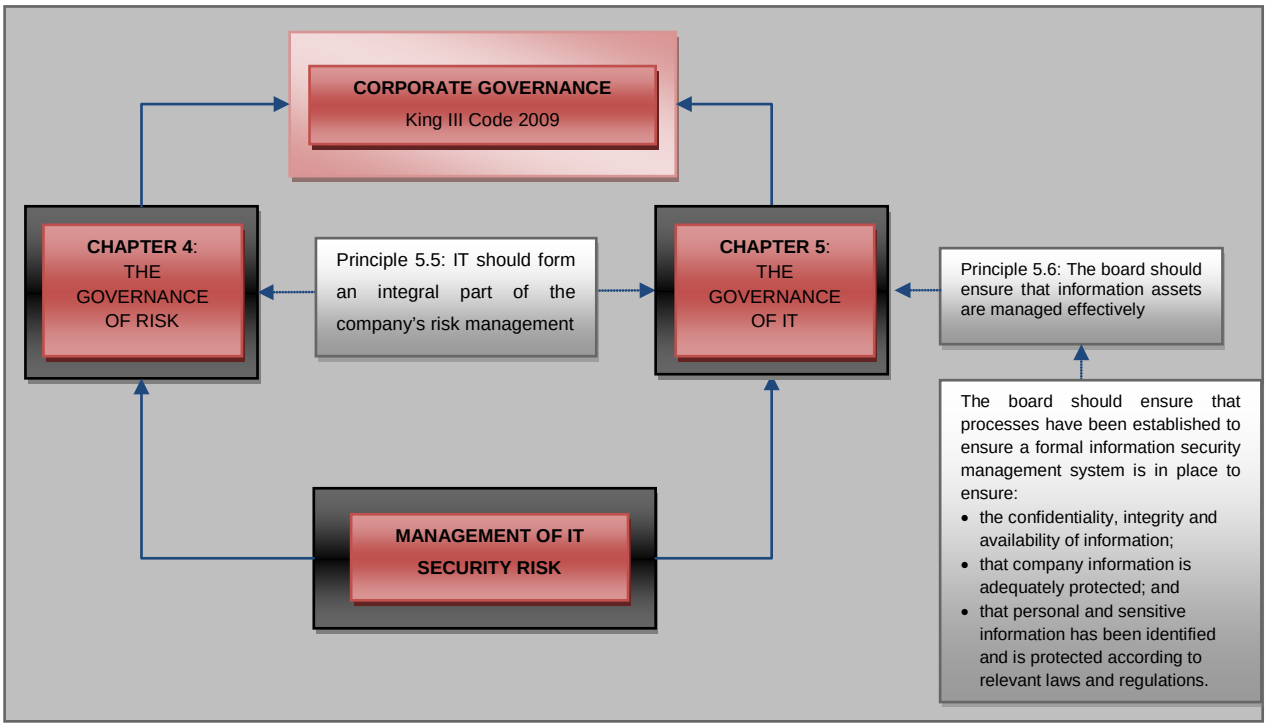

Figure 3.3 – The Foundation of IT Security Risk Management

According to the National Institute of Standards and Technology (NIST) (2010), the process of due care and due diligence for protecting IT assets is required to exercise a robust risk management process. This raises the need for IT security risk management (NIST, 2010).

Chowdhury, et al. (2012) demonstrated in their study that the significance of IT security is globally accepted and that it involves a risk management process to justify the investment for IT security measures in order to support the IT security risk management process throughout all stages of IT. IT security is considered a risk management strategy and should be addressed as one of the many key risk areas (Jahankhani & Nkhoma, 2009). An effective IT security risk evaluation considers both organisational and technological issues, examining how people use their organisation's IT infrastructure on a daily basis (Alberts, et al., 2003).

Figure 3.3 demonstrated that IT security risk management embodies the primary goals of corporate governance, risk management, and IT governance. The ultimate goal of the process of IT security risk management is to make senior management within an organisation aware of possible risks including threats and consequences (NIST, 2010). IT security risk management guides organisations towards the adoption of a set of

actions which can bring the overall IT security risk to an acceptable level, thereby realising the return on security investment (Ketel, 2008).

Having reviewed the key principles of well-founded frameworks and standards for corporate governance and risk management (i.e. King III Code:2009, ISO 31000:2009), it is safe to conclude that a typical IT security risk management framework should be guided by the following principles:

- The starting point in the process of IT security risk management is to categorise IT assets as per their criticality to the organisation.
- The risk (likelihood and its impact) should be viewed holistically (i.e. from the perspective of the entire organisation, not only IT).
- The identified risks should have a business impact or quantifiable loss.
- The base of the evaluation of risk should encompass all kinds of risk, from minor IT security incidents to potentially catastrophic events.
- Once IT assets have been classified, IT security controls can be selected, implemented, assessed, authorised and then monitored on a periodic basis.

Now that the foundation of IT security risk management has been discussed, it is important to analyse the selected best practice frameworks and standards in order to evaluate their strengths and weaknesses for IT security risk management in the next section.

3.4. IT SECURITY FRAMEWORKS AND STANDARDS

This section describes some of the common IT security frameworks and standards used within South African financial institutions (Amsenga, 2005; Maphakela, 2008). It is important to note that there are many other IT security frameworks and standards within the current body of knowledge developed by local governments within different European countries such as Austrian IT Security Handbook; Cramm Tool developed by British Central Communication and Telecommunication Agency; Dutch A&K Analysis; Expression des Besoins et Identification des Objectifs de Sécurité (Ebios) from France;

and Information Security Assessment & Monitoring Method (ISAMM) from Belgium (ENISA, 2005). However, these frameworks and standards are beyond the scope of this study, as this study examines the common IT security frameworks and standards used within South African financial institutions.

The frameworks and standards selected are Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); ISO 27001/2; Control Objectives for Information and related Technology 5 (COBIT 5); Information Technology Infrastructure Library version 3 (ITIL v3); and Information Security Forum Standard of Good Practice (ISF SoGP). These frameworks and standards were selected because they provide a focused scope that is exhaustive and they are commonly used within South African financial institutions.

OCTAVE is an IT security risk management framework (Alberts, et al., 2003). COBIT 5 and IT Infrastructure Library (ITIL) are categorised as IT governance frameworks even though COBIT 5 is more strategic and ITIL is more operational; however, both of them have IT security as sub-components (ITSMF, 2007; ITGI, 2012). Similarly, ISF SoGP and ISO 27001/2 are purely IT security standards with the objective of assisting organisations in managing IT security adequately (ISO/IEC 27001, 2007; Chaplin & Creasy, 2011).

Although the discussed frameworks and standards approach the subject of IT security differently, their ultimate goal is to reduce IT security risk to an acceptable level as per the organisation's risk appetite. The analysis presented in this section explores the selected frameworks and standards with emphasis on their strong characteristics, which are consolidated in developing the proposed ITSRB approach.

The following sections discuss the selected frameworks and standards (i.e. OCTAVE, ISO 27001, COBIT 5, ITIL, and ISF SoGP) in detail to highlight their characteristics, key strengths and shortcomings.

3.4.1. OCTAVE

OCTAVE is a process-driven framework that enables organisations to understand, assess and address their security risks from the organisation's perspective by identifying, prioritising and managing security risks (Panda, 2009). OCTAVE is described as a self-directed approach that people from an organisation can use to administer and direct security risk evaluation activities (Marek & Paulina, 2006).

3.4.1.1. Characteristics of OCTAVE

OCTAVE is an IT security risk management framework (Alberts, et al., 2003). OCTAVE is a systematic approach because it enables people within an organisation from different dimensions (i.e. top management, middle management and operational staff) to identify security issues within their immediate areas (Marek & Paulina, 2006). The ability for IT security to be managed at various levels tends to improve an entire organisation's security posture without placing unnecessary reliance on outside experts and vendors (Alberts, et al., 2003).

Alberts, et al. (2003) point out that for an organisation to understand its security needs, OCTAVE is ideal because it is a holistic risk based strategic assessment and planning technique for security. OCTAVE emphasises that the level of risk tolerance for an organisation should be determined first before the security strategy in order to ensure the highest possible level of protection, without hindering business activities (Marek & Paulina, 2006). OCTAVE allows a balance to exist between the protection of critical information assets and the cost of providing protective and detective controls (Albert & Dorofee, 2001; Alberts, et al., 2003).

OCTAVE strives to balance three aspects: operational risk, security practices, and technology (White, 2012). Balancing risk, security and technology ensures that all other aspects outside the IT environment are considered during an OCTAVE assessment (Alberts, et al., 2003; White, 2012). In principle, the risk management activities are built as foundational activities during the OCTAVE assessment (Alberts, et al., 2003). Unlike the typical technology-focused assessments, which are targeted at technological risk and focused on tactical issues, OCTAVE is targeted at organisational risk and focused on strategic, practice-related issues (Alberts & Dorofee, 2001).

OCTAVE has four major components: Asset, Threat, Vulnerability, and Impact (Panda, 2009). A security risk evaluation must have an accountability of all of the four major components of OCTAVE (Alberts, et al., 2003; Whitman & Mattord, 2005; Panda, 2009).

OCTAVE is organised into three phases to assess the organisational view, the technological view and the actual security risk analysis process. The OCTAVE framework is depicted in Figure 3.4.

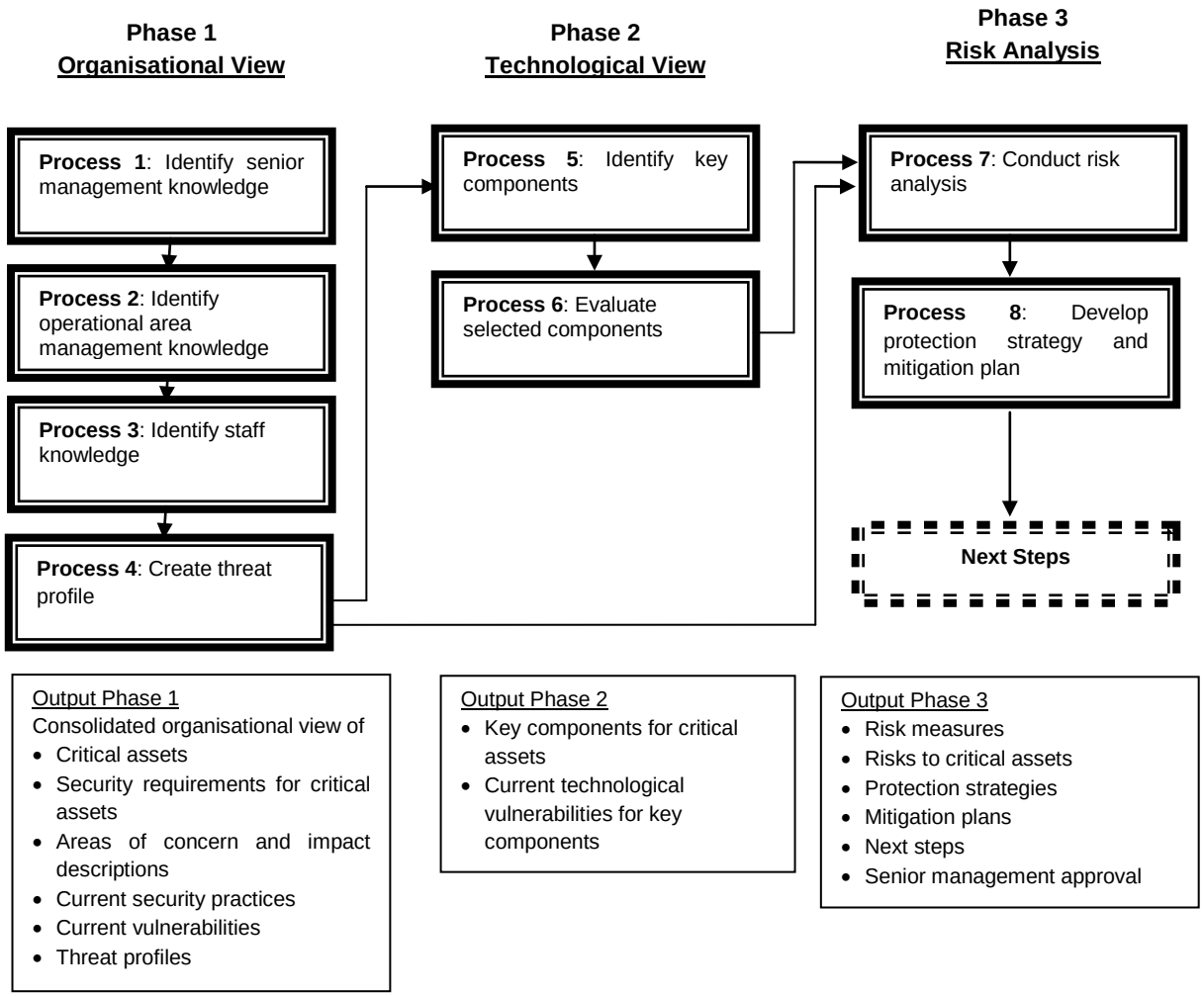

Figure 3.4 – The OCTAVE Phases

Source: Panda (2009)

Phase 1: Build asset-based threat profiles – This is an organisational evaluation. The analysis team determines what is important to the organisation (information-related

assets) and what is currently being done to protect those assets (Panda, 2009). Important assets to the organisation are then selected; IT security requirements and threats for each of the organisational assets are described (Alberts & Dorofee, 2001). The output of this phase is an IT security threat profile for each important organisational asset (Panda, 2009).

Phase 2: Identify infrastructure vulnerabilities – This is an evaluation of IT. The network access paths and classes of IT components related to each critical asset are examined (Alberts & Dorofee, 2001). The output of this phase provides a view of the potential vulnerabilities of IT assets relating to organisational assets (Panda, 2009).

Phase 3: Develop security strategy and plans – During this part of the evaluation, a risk analysis of the identified IT security risks is conducted (Alberts & Dorofee, 2001). The output of this phase is an IT security strategy which details the IT security mitigation plans to address the risks to critical assets, based on an analysis of the information gathered (Panda, 2009).

3.4.1.2. Advantages of OCTAVE

OCTAVE is self-directed

This means that the organisation's personnel are involved in the decision-making process (Marek & Paulina, 2006). The OCTAVE method also emphasises that the analysis team can add personnel (i.e. subject matter experts to provide further detail) as and when needed during assessment workshops (White, 2012).

OCTAVE is systematic and context-driven

OCTAVE develops risk evaluation criteria based on operational risk tolerances from both strategic and operational areas (Panda, 2009). Developing risk evaluation criteria aids in identifying vulnerabilities and threats of importance, and evaluating potential consequences to the organisation should the risk materialise (White, 2012).

OCTAVE is a risk based approach

As previously discussed, information and IT are essential to organisations, and ensuring adequate protection to them is important to organisations' missions (Whitman & Mattord, 2005). There is a need for organisations to focus on their most important information assets when making decisions about protecting them in order to achieve optimal return on security investments (Whitman & Mattord, 2005). Adopting security controls to protect information assets without proper assessment of risks will either overprotect assets, making security a hindrance to business operations, or under protect assets, resulting in the exposure of business-critical assets to threats (Panda, 2009). OCTAVE allows organisations to balance the protection of critical information assets against the costs of providing protective and detective controls (Whitman & Mattord, 2005; Panda, 2009).

The benefits associated with the use of OCTAVE are indescribable and demonstrate value to organisations by ultimately saving money in the long run (Whitman & Mattord, 2005; Panda, 2009). Having reviewed the key strengths of OCTAVE, it is also important to discuss its shortcoming, which may present challenges when OCTAVE is used within organisations.

3.4.1.3. Disadvantages of OCTAVE

Dedication of top management to the assessment exercise

Time invested in conducting an OCTAVE assessment is significant (White, 2012). For organisations with a low maturity level towards risk, the assessment may be perceived to be interfering with normal business operations (Whitman & Mattord, 2005). Different departments within organisations are all about meeting deadlines and delivering tangible results to the business; therefore, something that anticipates adding value without immediate tangible results may derail the end goal of implementing OCTAVE (White, 2012).

Implementation, monitoring and control

OCTAVE only focuses on identification, analysis and planning of the risk management activities. Once these activities have been completed, the OCTAVE assessment is complete (Whitman & Mattord, 2005; White, 2012). The implementation of the proposed controls is left to the management teams (White, 2012). This might mean that the efforts put into the OCTAVE exercise are neglected if the implementation, monitoring and control assessment exercises are not conducted on a periodic basis (Whitman & Mattord, 2005; White, 2012).

Misinterpretation of the information gathered

There is often a chance of information gathering being misunderstood due to many factors such as time or language barriers (White, 2012). If those in the OCTAVE analysis team are not experienced enough, they may end up gathering wrong information, thus making this exercise superfluous (White, 2012).

3.4.2. ISO 27001

ISO 27001 is an international standard for information security cited as ISO/IEC 27001:2013, which is superseded by ISO/IEC 27001:2005 (ISO/IEC 27001, 2013). ISO 27001 was developed by ISO and IEC, which are international bodies whose members are subject matter experts responsible for participating in developing international standards through technical committees (ISO/IEC 27001, 2013). The primary goal of ISO 27001 is to provide its users with guidelines on security controls which can be applied within an organisation to manage risk associated with IT security (ISO/IEC 27001, 2013). ISO 27001 recommends a risk based security management system that is developed to ensure that organisations select and operate adequate and proportionate security controls to protect organisational assets from security threats (ISO/IEC 27001, 2013).

3.4.2.1. Characteristics of ISO 27001

Both ISO 27001 and ISO 27001 are subsets of the ISO 27000 series. ISO 27001 encompasses process descriptions which may be used to select and implement

controls; and ISO 27002 contains a comprehensive list of controls. ISO 27001 is used as a model to build an Information Security Management System (ISMS). The ISMS is a structured approach to managing organisational information assets by recommending security controls (ISO/IEC 27001, 2013). The ISMS stipulates a risk based security management system that is designed to ensure that organisations select and operate adequate and proportionate security controls to protect information assets (Pelnekar, 2011; Verheul, 2011).

The ISMS framework illustrates the components that are needed to ensure a holistic risk based view while enabling benefits from business opportunities (ISO/IEC 27001, 2013). Establishing an ISMS framework is a strategic decision and shows management commitment to good governance through managing and mitigating information and IT security risk (ISO/IEC 27001, 2013).

ISO 27001 recommends that senior management within an organisation should systematically examine security risks, design and implement security controls, and adopt the controls using a risk based approach (ISO/IEC 27001, 2013). ISO 27001 comprises 11 domains, 39 control objectives and over 130 controls.

In applying the recommended controls, internal and external factors including outsourced IT services should be considered (ISO/IEC 27001, 2013). Considering external factors will ensure that security requirements for interfaces and dependencies of an organisation with third parties are also accounted for (ISO/IEC 27001, 2013).

Verheul (2011) states that the responsibility for security within the organisation should not be placed solely on information security personnel or the IT department, as they typically do not know all the characteristics of the business processes. The responsibility of security should be placed at the senior management level that is responsible for the organisations as a whole as well as the business process (Verheul, 2011).

Furthermore, ISO 27001 enables organisations to benchmark against competitors, thereby allowing organisations to provide relevant information about security through demonstration of security due diligence to vendors and customers if necessary

(Pelnekar, 2011). The ISO 27001:2005 version emphasised the Plan-Do-Check-Act The ISO27001:2005 version emphasised the Plan-Do-Check-Act (PDCA) cycle (Figure 3.5) also known as the Deming cycle which allows for management to know how far and how well the organisation has progressed during each cycle of implementation (ISO/IEC27001, 2005; Pelnekar, 2011; Verheul, 2011).

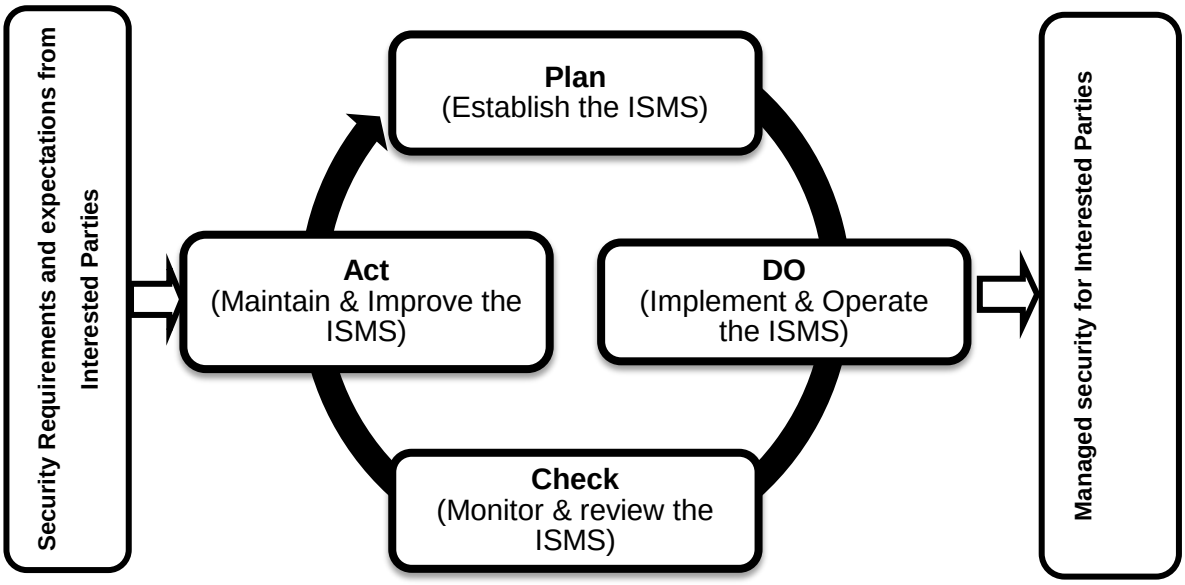

Figure 3.5 – The Plan-Do-Check-Act Process

Source: ISO/IEC 27001 (2005)

The PDCA cycle for ISO 27001 is described as follows:

Plan: The planning process of ISO 27001 involves identifying business objectives while involving management of an organisation to get support (ISO/IEC 27001, 2005). Afterwards, the scope of implementation is prioritised and selected (Pelnekar, 2011). A method of risk assessment is then defined and executed, ranking assets according to risk classification and selecting adequate controls from the ISO 27002 standard (ISO/IEC 27001, 2005; Pelnekar, 2011; Verheul, 2011).

Do: The actual risk management activities are carried out in this phase (ISO/IEC 27001, 2007; Pelnekar, 2011). A risk treatment plan is executed, hence setting up and implementing policies and procedures to control risk, as well as allocating resources thereof (ISO/IEC 27001, 2005).

Check: This phase involves monitoring activities of the implemented ISMS (Verheul, 2011). An internal review of the performance of implemented processes and controls is conducted (Pelnekar, 2011; Verheul, 2011).

Act: The effectiveness of the controls is reviewed by conducting periodic reassessments with the objective of adjusting the ISMS for continual improvement (Verheul, 2011).

3.4.2.2. Advantages of ISO 27001

ISO 27001 is globally recognised

Implementing ISO 27001 can enable organisations to benchmark against competitors and to provide relevant information and a level of assurance about IT security to vendors and customers (ISO/IEC 27001, 2013). Furthermore, proper implementation of ISO 27001 can promote compliance with laws and regulations (Verheul, 2011; Pelnekar, 2011; Susanto, et al., 2012).

ISO 27001 can increase business and IT alignment

Most organisations regard security as a technology issue that security professionals can deal with (Pelnekar, 2011). One of the first things to accomplish when implementing ISO 27001 is to identify objectives of the organisation prior to creating a vision for security (Pelnekar, 2011). This process will ensure that ISO 27001 is aligned with both the business and IT objectives, thereby making certain that the security pain points are addressed in a prioritised manner that provides value to the business (Calder, 2013). It therefore becomes easier to communicate security decisions to business and show the value of security risk reduction because security becomes an integral part of business operations (Pelnekar, 2011; Calder, 2013). In turn, the responsibility of information security will shift to the business rather than IT (Pelnekar, 2011; Calder, 2013).

Improved effectiveness of information security

ISO 27001 provides tried-and-tested best practice guidance (Susanto, et al., 2012). The regular checkpoints via the PDCA allow for organisations to assess their security posture, thereby providing a mechanism for improving what could have been missed in the previous iterations (Pelnekar, 2011; Calder, 2013).

Better awareness of security across an organisation

Implementation of ISO 27001 can raise security awareness across the organisation, from senior management to junior staff (Calder, 2013). The organisations' employees will be aware of their roles and responsibilities in looking after the organisations' security risk as they are provided with the correct responsibilities of security (Susanto, et al., 2012; Calder, 2013).

Competitive advantage

Organisations across the globe are now concerned with information protection (Susanto, et al., 2012). If an organisation intends to outsource some of its services to external vendors, it would go for the vendor that has accreditation such as ISO 27001 (Calder, 2013). Accreditation to ISO 27001 provides the organisation with competitive advantage against other organisations within the same industry because it demonstrates the level of commitment by management to security (Susanto, et al., 2012).

3.4.2.3. Disadvantages of ISO 27001

Limited expertise within organisations' resources

The skill set within the security industry is limited (Pelnekar, 2011). Imprecise understanding of the ISO 27001 standard and its requirements makes it difficult to envisage what the end result should be (Susanto, et al., 2012). A significant number of ISO 27001 implementations fail due to the fact that the implementation is performed by

people with wrong skill sets and not external specialist consultants who come at a high cost (Susanto, et al., 2012; Calder, 2013).

Scope of implementation

ISO 27001 is a considerably large standard and cannot be implemented all at once (Susanto, et al., 2012; Calder, 2013). Implementation requires a phased approach to ensure that the correct scope is selected and focused on (Calder, 2013). Organisations that prefer using phased approaches to implementing projects might see ISO 27001 as a "big elephant" and then opt for other standards (Susanto, et al., 2012).

Cost and effort of implementation

The associated costs and project length that come with implementing ISO 27001 may be seen as a big factor and need to be taken into consideration (Pelnekar, 2011). Keeping up with industry trends may be regarded as a burden, as many people see standards such as ISO 27001 as a "nice-to-have" (Calder, 2013).

3.4.3. COBIT 5

Control Objectives for Information and related Technology (COBIT) is an IT governance framework that provides best practice processes for different IT domains (ITGI, 2012). The COBIT framework was defined and created by a group of experts in various areas of IT with a concerted effort of creating a framework which could allow organisations to realise the benefits of their IT investment (ITGI, 2012). The COBIT framework was initially released in 1996 (ITGI, 2012). The revised version (i.e. COBIT 4.1) was later released in 2007 and has now been improved with the latest version (i.e. COBIT 5), which was released in 2012. For the purpose of this study, COBIT 5 will be focused on, as it encompasses the principles of previous COBIT versions.

COBIT 5 is developed in a way that allows for its users to meet the current needs of stakeholders by aligning to the latest thinking of corporate governance and IT management principles (ITGI, 2012). As previously stated, the COBIT 5 framework uses COBIT 4.1 as a foundation and incorporates the Val IT and Risk IT frameworks. The objective of Val IT is to assist organisations with deriving business value from IT

investments through effective IT governance practices (ITGI, 2012). The Risk IT framework provides a holistic view of risks related to the use of IT and recommends a thorough treatment of risk to operational issues (ITGI, 2012).

3.4.3.1. Characteristics of COBIT 5

The primary idea behind COBIT 5 is to explicitly provide organisations with a strong foundation of processes which should be performed within the IT environment (ITGI, 2012). The objective is achieved through balancing benefit realisation while optimising risk levels (ITGI, 2012). The ultimate goal of COBIT 5 is to enable organisations to optimise their IT-enabled investments, thus ensuring service delivery to the business as well as providing tools to measure against when things go wrong (ITGI, 2012). COBIT emphasises that the IT strategy should be derived from the business strategy (ITGI, 2012). In addition to that, the commitment of senior management into embedding the COBIT 5 framework is fundamental to its success (ITGI, 2012).

COBIT 5 emphasises the importance of measuring performance through setting and monitoring objectives regarding what the IT processes need to deliver (ITGI, 2012). Additionally, performance measurement provides organisations with a way of providing transparency of IT cost, value and risks, which have proven to be drivers for IT governance (ITGI, 2012).

Understanding roles and responsibilities for each process is important and forms the basis for effective governance (ITGI, 2012). COBIT 5 recommends a RACI model (i.e. Responsible, Accountable, Consulted and Informed) for each process within its domains (ITGI, 2012). Responsibility refers to the person who executes a task (ITGI, 2012). Accountability refers to the person who provides direction and authorises an activity (ITGI, 2012). The Consulted and Informed roles are two roles played by individuals who are involved and support the processes (ITGI, 2012).

COBIT 5 advocates that organisations must implement fit-for-purpose IT processes in a way that will satisfy governance and management requirements, as depicted in Figure 3.6.

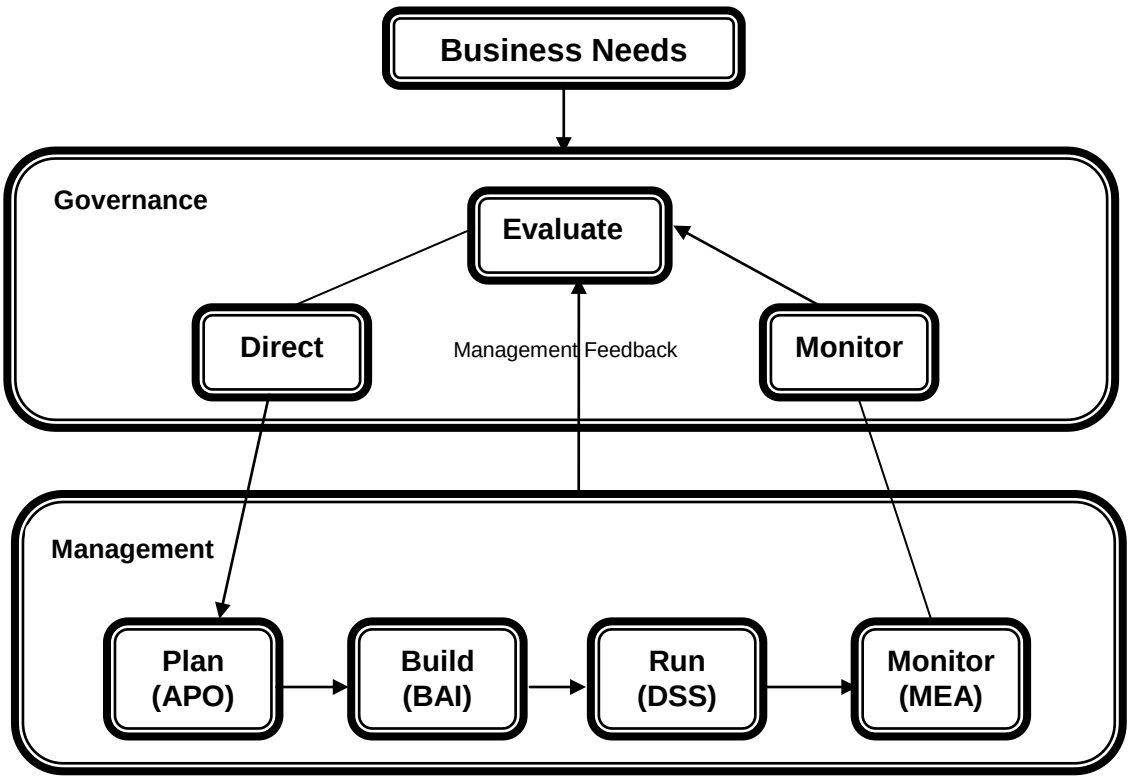

Figure 3.6 – COBIT 5 Process Reference Model

Source: ITGI (2012)

Business requirements are deemed to be the drivers of the COBIT 5 framework, as they prescribe IT requirements (ITGI, 2012).

3.4.3.1.1. Governance

The goal of the governance component is to ensure that requirements of IT are assessed to determine balanced organisational objectives that need to be achieved by IT (ITGI, 2012). The governance domain consists of three basic processes: evaluate, direct, and monitor.

The evaluate component ensures that business requirements are assessed from a governance perspective, ensuring that IT delivery is adequate (ITGI, 2012). The direct component ensures that IT activities are prioritised as per the business requirements

and are performed adequately (ITGI, 2012). The monitor component involves providing oversight to the execution of IT activities, ensuring that any areas of improvement are recognised and improved upon (ITGI, 2012).

3.4.3.1.2. Management

The goal of the management component is to define, implement and execute plans to run monitoring activities set by the governance domain to achieve organisational goals (ITGI, 2012). The management component consists of four processes: Align, Plan and Organise (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA).

Align, Plan and Organise (APO): The process of “aligning, planning and organising” is about reviewing the IT resources and capabilities that the organisation has, determining the best way on how to utilise them, and devising a plan on how they will be used through a strategy (ITGI, 2012). Aligning ensures that IT requirements are aligned with the business requirements (ITGI, 2012). Planning provides the direction that IT should follow in a way that will appreciate the activities and risks within IT that need to be managed (ITGI, 2012).

Build, Acquire and Implement (BAI): This domain is concerned with the development or procurement and implementation of IT solutions which are harmonised with the business requirements (ITGI, 2012). The solutions can be developed internally or can be obtained externally from third parties, but the primary goal is to ensure that these solutions deliver the IT strategy that is aligned with the business strategy (ITGI, 2012).

Deliver, Service and Support (DSS): This domain is concerned with the actual supply of the IT services which have been acquired in line with business operations (ITGI, 2012). Failure of the IT services delivered might result in dire consequences for the business operations (ITGI, 2012). The requirement to ensure systems security, which is a core focus of this study, is found in this domain.

Monitor, Evaluate and Assess (MEA): The monitor, evaluate and assess domain can be seen as a reflection process for the IT environment (ITGI, 2012). It is focused on assessing what works and what does not work within the IT environment (ITGI, 2012).

The assessment emphasises on performance monitoring of other processes, internal controls, governance, as well compliance with regulatory bodies (ITGI, 2012).

Across the five domains, COBIT 5 comprises 37 IT processes that can generally be used to verify completeness of responsibilities and IT activities (ITGI, 2012). In some instances, certain processes might not apply or they might be combined with other processes; each organisation should use COBIT as appropriate to its internal IT environment (ITGI, 2007).

3.4.3.2. Advantages of COBIT

Making a link to the business requirements

IT is regarded as the business enabler, and the IT strategy is driven by the business strategy. COBIT 5 allows for executives within organisations to have better confidence in the organisations' reliance on the IT systems and the information produced by those systems, thereby giving them more confidence about their positive return on their IT investments (Gartner, 2012).

Organising IT activities into a generally accepted process model

COBIT 5 provides executives within an organisation with a mechanism to better understand how to direct and manage their organisations' IT use and the standard of good practice to be expected from IT service providers (Gartner, 2012). This is because the domains and process objectives for COBIT 5 are grouped in a way that is generally accepted globally. COBIT 5 therefore provides a common language for business executives to communicate goals, objectives and results with audit, IT and other professionals (ITGI, 2012).

Identifying the major IT resources to be leveraged

COBIT 5 provides organisations with the mechanism to direct and oversee all IT-related activities (Gartner, 2012). Once COBIT has been implemented effectively, it becomes easier to prioritise as well as measure performance on the IT resources which provide a platform to be used when business strategic decisions are made. This way, the

organisation will find a balance between leveraging off underutilised and overutilised IT resources throughout their life cycle (ITGI, 2012).

3.4.3.3. Disadvantages of COBIT

High degree of abstraction

COBIT 5 does not include concrete methods and guidelines assisting organisations to optimally accomplish its benefits (Zhang & Le Fever, 2013). This is because COBIT 5 is more of a governance framework rather than a process framework (Zhang & Le Fever, 2013). COBIT 5 focuses on what organisations need to do and not how they do it. This implies that as a single framework used within an organisation for IT, there might be gaps during implementation of COBIT 5 because it provides a broad coverage and minimal depth of how things should be done (Zhang & Le Fever, 2013).

Poor focus on IT

Because COBIT 5 is based on many existing practices, it is referred to as the 'integrator', bringing unrelated practices under one umbrella. With COBIT 5, there is a lack of implementation guidelines and proven benefits thereof (Gartner, 2012; Zhang & Le Fever, 2013). COBIT 5 sets the standard by focusing on a process-based system and on the risks generated by the utilisation of IT; it does not set the standard from the basic IT services (Zhang & Le Fever, 2013).

3.4.4. ITIL

IT Infrastructure Library (ITIL) is a framework that provides best practice guidance for IT service management (ITSMF, 2007). IT service management is described by ITSMF (2007) as a means of delivering value to customers by providing them with organisational capabilities that customers need in order to utilise the information that they own. ITIL recommends that organisations must recognise IT services as crucial strategic assets and ensure that they invest adequate levels of resources into their support, delivery and management, as well as the IT systems that underpin them (ITSMF, 2007).

3.4.4.1. Characteristics of ITIL

Under ITIL, information is regarded as one of the most important strategic resources that any organisation has to collect, analyse, produce and distribute because all organisations that use IT depend on IT to be successful (ITSMF, 2007). The primary objective of ITIL is to assist organisations to actively support the business (ITSMF, 2007). Supporting the business is achieved by ensuring that IT services underpin the business needs and processes enabling IT to act as an agent for change in order to facilitate business transformation (Mohamed, et al., 2008).

IT service management views each IT service, process or infrastructure component as an element that has a life cycle (ITSMF, 2007). The capabilities of IT service management are applied to the entire life cycle of ITIL, namely, service strategy, service design, service transition, service operations, and continual service improvement (ITSMF, 2007). Therefore, ITIL basically provides a framework for the governance of IT and focuses on the continual measurement and improvement of the quality of IT services delivered, from both a business and customer perspective (ITSMF, 2007).

Figure 3.7 summarises the ITIL service life cycle stages and the associated sub-processes of each phase.

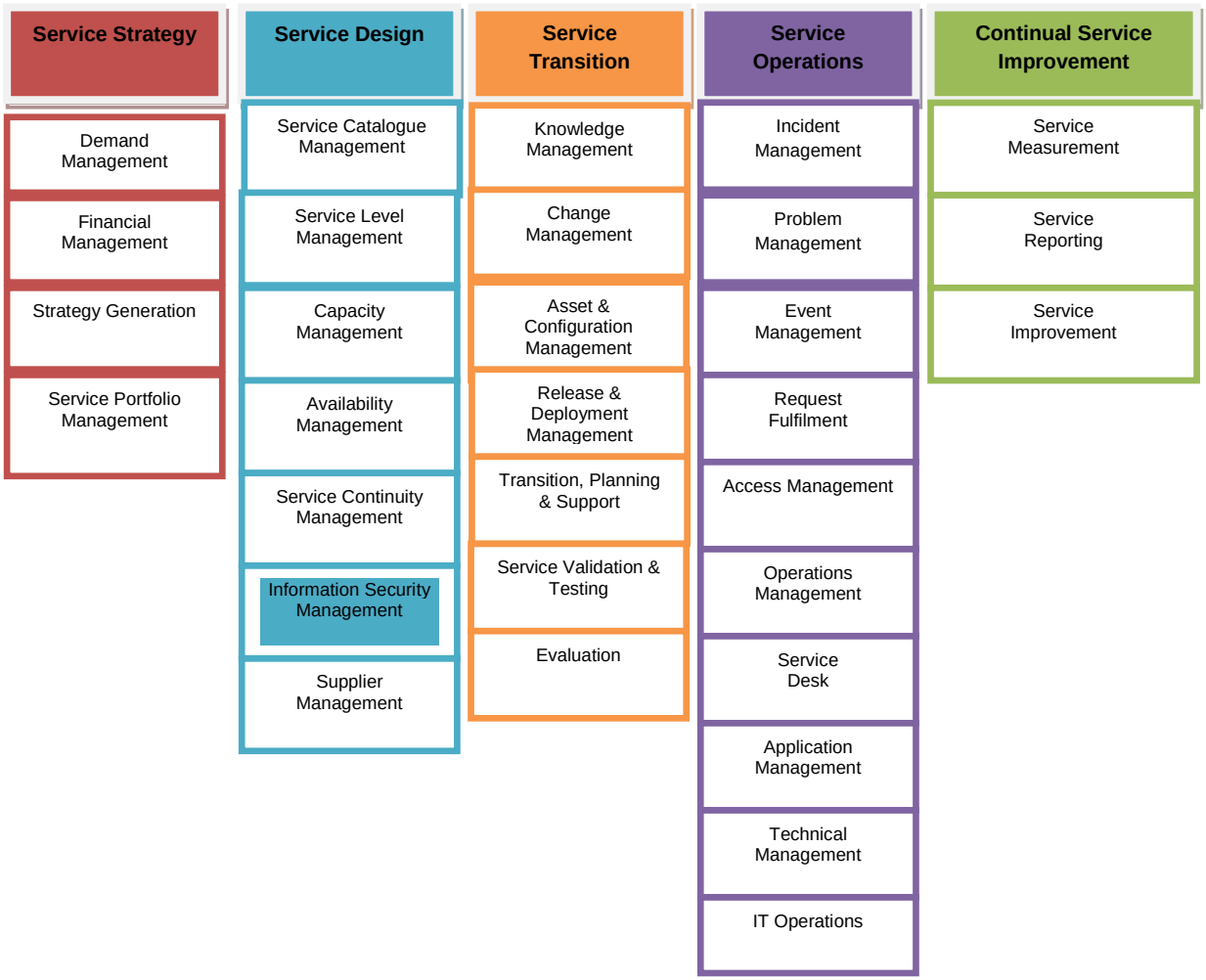

Figure 3.7 – The Service Life cycle Stages and Activities

Source: ITSMF (2007)

Service Strategy: Service strategy refers to the approach that will be used by IT service providers to service their customers (ITSMF, 2007). Within the ITIL framework, service strategy sits at the core of the life cycle because it sets out guidance on how customers and service providers should operate (ITSMF, 2007). In order to satisfy customers, IT service providers must understand who their customers are; what they need; why those needs occur; which market they operate in; what their perceived value is; how will value be measured; and how service performance will be measured (ITSMF, 2007). The IT service strategy cannot be defined in isolation from the overarching organisational strategy because the main idea is to deliver services that will ultimately fulfil that organisation's strategic purpose (ITSMF, 2007). Service strategy consists of four processes (ITSMF, 2007), namely, demand management, financial management, strategy generation and service portfolio management.

Service Design: Service design is concerned with the design of appropriate and innovative IT services including service architectures, processes, policies and documentation (ITSMF, 2007). IT services for ITIL are designed in a way that assists organisations in meeting both current and future agreed business requirements (ITSMF, 2007). The key activities of service design are service catalogue management, service level management, capacity management, availability management, service continuity management, information security management, and supplier management (ITSMF, 2007).

Information security management, which is the focus area of this study, is concerned with ensuring that the confidentiality, integrity and availability of services delivered to the business are maintained throughout the service life cycle (ITSMF, 2007). Information security management assists in delivering corporate governance framework goals (i.e. responsibilities exercised by executive management ascertaining that IT security risks are being managed adequately) (ITSMF, 2007).

Service Transition: Service transition aims to ensure that designed services required by the business are put into operational use (ITSMF, 2007). In cases where business circumstances have changed, modifications are carried out in the service transition stage (ITSMF, 2007). Service transition focuses on implementing services which are robust and can operate under unfavourable circumstances (ITSMF, 2007). Sub-processes of service transition are change management; service asset and configuration management; knowledge management; transition planning and support; release and deployment management; service validation and testing; and evaluation (ITSMF, 2007).

Service Operations: Service operations stage is primarily concerned with making sure that agreed levels of service are delivered to the business and that applications, technology and infrastructure are managed in a way that supports delivery of the services (ITSMF, 2007). It is only during this stage of the life cycle that the business can actually realise the value of the services which are delivered by the IT service provider (ITSMF, 2007). Service operations stage consists of ten key sub-processes (ITSMF, 2007), namely, incident management; problem management; event management;

request fulfilment; access management; operations management; service desk; application management; technical management; and IT operations.

Continual Service Improvement: This process is concerned with continual evaluation and improvement of the quality of the IT services across the service life cycle and underlying processes (ITSMF, 2007). Principles, practices and methods from quality management are combined, working to improve each stage in the service life cycle as well as the services, processes, technology and related activities (ITSMF, 2007). Continual service improvement is an iterative activity which assesses the vision of IT through the business objectives (ITSMF, 2007). Moreover, the continual service improvement stage assists in assessing the performance of IT through baseline assessments and measurable targets (ITSMF, 2007). Once performance targets have been set, processes to ensure that targets are achieved are implemented in this stage of ITIL (ITSMF, 2007). Continual service improvement consists of three sub-processes: improvement process, service measurement, and service reporting (ITSMF, 2007). The section that follows discusses the key strengths of ITIL.

3.4.4.2. Advantages of ITIL

Increased user and customer satisfaction

When IT services are explicitly defined, measuring the service levels related to the delivered services becomes more manageable, thus improving customer satisfaction (ITSMF, 2007).

Improved service availability

Managing the delivered IT service levels closely assists in ensuring that any service interruptions are detected swiftly, which leads to high availability (ITSMF, 2007).

Improved decision-making and optimised risk

The comprehensive service life cycle ensures that all aspects relating to each and every IT service are taken into account during design, analysis and operation, leading to reduced risk and improved decision-making (ITSMF, 2007).

Improved time to market for new products and services

Service providers have the opportunity to design and implement new services when the IT environment is scalable and well defined (ITSMF, 2007).

Even though ITIL provides various benefits, it is important to note the associated shortcoming that it possesses.

3.4.4.3. Disadvantages of ITIL

Failure to fully understand the breadth and depth of ITIL leads to implementation failures

To implement the ITIL framework successfully, service provider teams, as well as customers, need to understand the framework and the impact of the framework across people, process and technology (ITSMF, 2007). Unfortunately, it is too challenging to reach such a level of understanding with all the people or at least the IT staff within an organisation (ITSMF, 2007).

Lack of top-level support may lead to implementation failures

This is the case with any framework; if there is no support from the top, there are very high chances that implementation of the framework might not be a success. The challenge is that ITIL has a high level of detail, which becomes a challenge for senior management, especially those with no IT background, to fully understand (ITSMF, 2007).

All ITIL-aligned processes and their performance require roles or individuals to be assigned to them

Depending on the size of the organisation, IT services can be complex, as each ITIL service requires a role assigned to it (ITSMF, 2007). Ensuring that all ITIL services have responsible roles, which many organisations fail to achieve, can be a daunting task (ITSMF, 2007).

ITIL is mostly IT-focused

ITIL is more orientated toward IT and therefore lacks focus on business aspects, resulting in resistance from the business community within organisations (ITSMF, 2007). Day-to-day operations of IT can become more about the processes than service delivery, as employees tend to focus on ensuring that processes are there, as opposed to delivery to the business (ITSMF, 2007).

3.4.5. The ISF Standard of Good Practice

The Information Security Forum (ISF) Standard of Good Practice (SoGP) for information security is a globally recognised standard that provides users with practical guidance on information security and information risk-related aspects (Chaplin & Creasy, 2011). Although the focus of this study is on IT security, the ISF SoGP is still regarded as vital to this study because information is regarded as a significant IT asset. The ISF SoGP addresses information security from a business perspective, providing an ideal basis for assessing and improving information security arrangements within any organisation (Chaplin & Creasy, 2011).

The ISF SoGP is globally recognised because it is defined and created by information security experts around the world (Chaplin & Creasy, 2011). Furthermore, the ISF SoGP is defined in a way that enables compliance with other recognised frameworks and standards such as ISO 27001 and COBIT. Because of this aspect, the ISF SoGP allows users to validate information security arrangements with external suppliers in a seamless manner (Chaplin & Creasy, 2011).

3.4.5.1. Characteristics of the ISF SoGP

Because the ISF standard of good practice guides its users in defining policies, standards and procedures for information security, it provides a basis for both detailed and high-level information security assessment (Chaplin & Creasy, 2011). Information security assessment is achieved by first assessing the business impact, followed by a threat and vulnerability assessment, and ending with a control selection (Chaplin & Creasy, 2011). Further, the ISF standard of good practice is divided into four

categories, namely, security governance, security requirements, control framework, and security monitoring and improvement (Chaplin & Creasy, 2011).

Security governance: The primary objective of security governance is to ascertain that an organisation's overall approach to information security supports high standards of governance (Chaplin & Creasy, 2011). To achieve the goal of security governance, an information security governance framework should be established by an organisation's governing body (Chaplin & Creasy, 2011).

An organisation's governing body should direct, monitor and communicate the information security governance framework within the organisation (Chaplin & Creasy, 2011). The governing body should ensure that information security is treated as a critical business issue and that there is a board-level executive or equivalent who is appointed to take overall responsibility for the information security governance framework (Chaplin & Creasy, 2011).

Appointing a board-level executive responsible for information security will assist organisations in ensuring that the information security governance framework is supported by the information security strategy as well as by an information security assurance programme (Chaplin & Creasy, 2011). Top-down management structure and mechanism for coordinating information security activities allow for organisations to have a clear direction that supports the information security governance approach (Chaplin & Creasy, 2011).

Security requirements: The security requirements domain is focused on information risk assessment and compliance (Chaplin & Creasy, 2011). Chaplin and Creasy (2011) emphasise that information is a key resource within any organisation and thus should be adequately managed. Implementation of information risk assessment activities is not comprehensive without a compliance process that ensures that there is adherence to legal and regulatory bodies as well as information privacy (Chaplin & Creasy, 2011).

Control framework: The control framework has a detailed list of the controls that should be applied throughout the organisation, including the IT environment, in order to achieve the goal of the information security governance framework (Chaplin & Creasy,

2011). The control framework provides guidance in the following areas: security policy and organisation; human resource security; asset management; business applications; customer access; access management; system management; technical security infrastructure; network management; threat and vulnerability management; incident management; local environments; desktop applications; mobile computing; electronic communications; external supplier management; system development management; system development life cycle; physical security and environmental security; and business continuity (Chaplin & Creasy, 2011).

Security monitoring and improvement: The security monitoring and improvement domain is solely focused on ensuring that there is continuous improvement in the posture of information security (Chaplin & Creasy, 2011). The two activities under security monitoring and improvement are security audit and security performance (Chaplin & Creasy, 2011). Security audit is concerned with assurance activities which aim to ensure that an acceptable level of assurance is achieved by the information security governance framework (Chaplin & Creasy, 2011). The security performance activity is focused on monitoring the performance of the information security governance framework across the organisation, ensuring that areas of improvement are identified, improvement plans are defined and then implemented (Chaplin & Creasy, 2011).

The ISF standard of good practice has some benefits that should be borne in mind.

3.4.5.2. Advantages of the ISF standard of good practice

Rigour

The ISF SoGP is comprehensive and, therefore, allows for a more effective process of identification of key risks and potential business impact (Chaplin & Creasy, 2011).

Efficiency

The ISF SoGP provides a detailed set of controls which cover the IT environment holistically, thus minimising the need to purchase additional repository of potential controls (Chaplin & Creasy, 2011).

Integration

The ISF SoGP is completely aligned with other globally recognised security frameworks and standards such as ISO 27001, COBIT and IRAM. This means that it can be incorporated easily within existing environments (Chaplin & Creasy, 2011).

Quality

The ISF SoGP provides a trusted standard set of controls for risk assessment across the organisation and enables selection of controls and implementation that is acceptable in accordance with the risk profile and risk appetite of the organisation (Chaplin & Creasy, 2011).

Having acknowledged the key strengths of the ISF SoGP, it is also important not to overlook shortcomings of this framework which may often present challenges when this framework is used within organisations.

3.4.5.3. Disadvantages of the ISF standard of good practice

Dependant on other frameworks and standards

The ISF standard of good practice is most valuable when it is used as a supporting framework and not as a stand-alone framework (Chaplin & Creasy, 2011). The ISF SoGP does not provide a comprehensive guide to users on “how” the recommended controls should be arranged within the organisation (Chaplin & Creasy, 2011).

Ambiguity

The ISF standard of good practice might be interpreted incorrectly by users because as much as it provides guidance as regards what controls should be implemented, it leaves the users with too much room for flexibility to interpreting how controls should be implemented (Chaplin & Creasy, 2011).

Compliance-focused

Compliance with regulatory bodies is an excellent thing; however, it does not help if one's organisation is considered compliant because controls exist while they are not operationalised effectively to address day-to-day operational challenges (Chaplin & Creasy, 2011).

3.5. CONCLUSION

This chapter commenced by defining the key concepts of information, IT and IT security in order to provide background information about the concepts used in this study. The two pillars of corporate governance, namely, risk management and IT governance were discussed in detail. Thereafter, an overview of IT security risk management, which is the basis for this study, was explained in depth. This was followed by a detailed analysis of the five IT security frameworks and standards, namely, OCTAVE, ISO 27001, COBIT, ITIL, and ISF SoGP. The analysis of each framework and standard was conducted by means of listing the objectives, characteristics, as well as the advantages and disadvantages of each framework.

The chapter that follows discusses threat modelling in order to understand the underlying concepts that may aid managing IT security risk.

4. MODELLING IT SECURITY THREATS

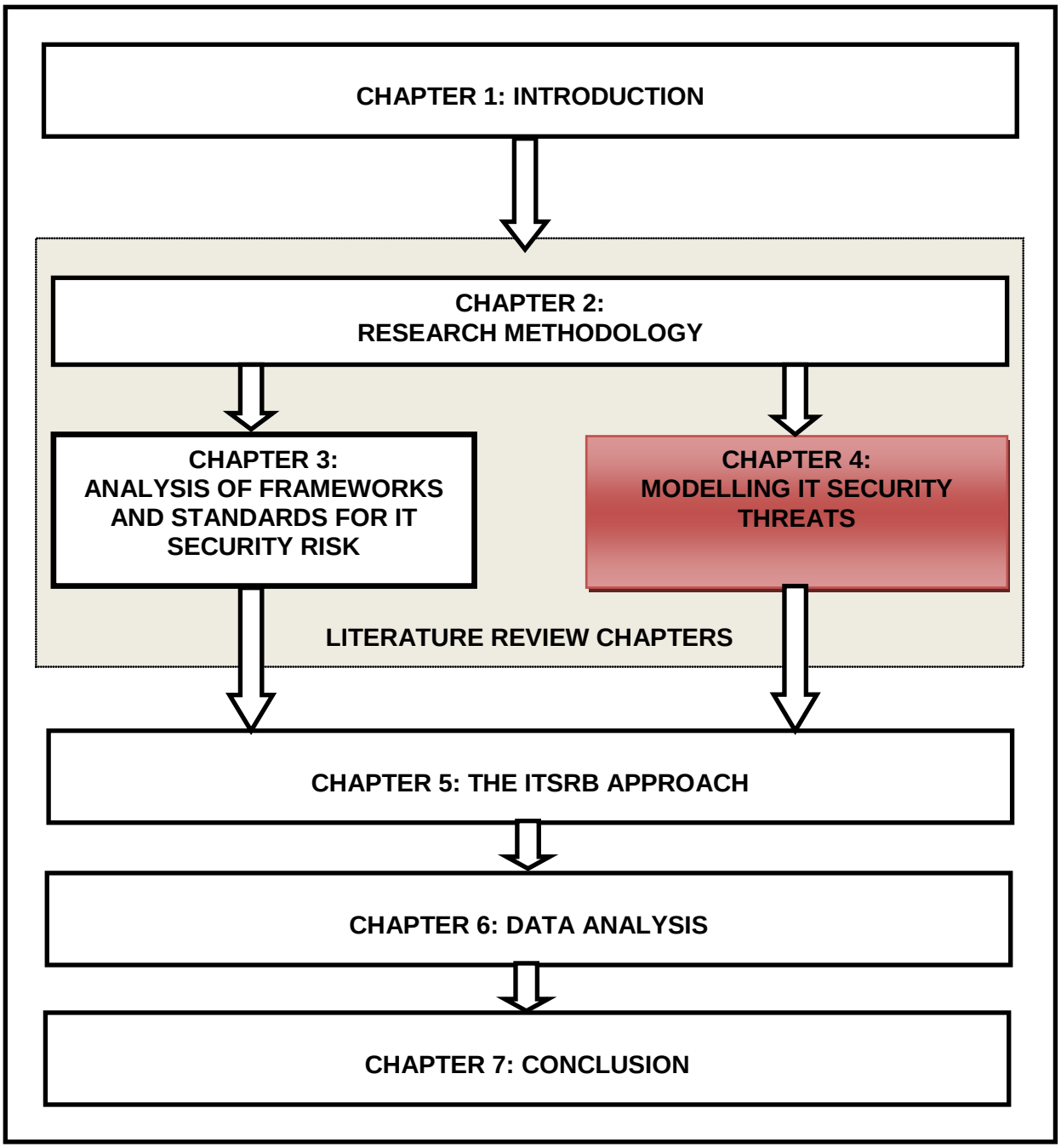

Figure 4.1 – Dissertation Layout: Chapter 4

4.1. INTRODUCTION

Management of IT security risk requires a holistic approach which ensures that both known and unknown risks are mitigated to an acceptable level (Hardy, 2012; Jouini, et al., 2014). IT systems are recurrently exposed to various types of threats which result in different types of damages (Jouini, et al., 2014). Damages are consequences resulting from exploited vulnerabilities, and examples include denial of service to systems, compromised integrity to information and information theft. When vulnerabilities exist in an IT system, a threat may be manifested through a threat agent using a particular penetration technique to cause undesired effects (Mougouei, et al., 2012).

The preceding chapter analysed frameworks and standards for IT security risk. The objective of this chapter is to define a basic threat modelling process which is incorporated in the IT security risk management process (Swiderski & Snyder, 2004). The threat modelling process described is iterative and systematic, providing a continuous proactive process for identification of threats and vulnerabilities (Meier, Mackman, Dunner, Vasireddy, Escamilla & Murukan, 2003). Section 4.2 presents the discussed threat modelling process developed by Meier, et al. (2003). Additionally, four best practice threat classification models are examined in Section 4.3 to demonstrate the importance of classifying threats for IT assets.

The output of this chapter is intended to enhance the proactive capability of the IT Security Risk Based (ITSRB) approach proposed in this study. The majority of the threat modelling processes found in this literature review is based at the application or solution level; however, the principles used are regarded as fundamental to the proposed ITSRB approach. Therefore, for the purpose of this study, an IT asset perspective encompassing the application view as well as the solution view is assumed.

4.2. THE THREAT MODELLING PROCESS

Threat modelling process is an approach used for evaluating the security of an IT asset, thereby identifying, quantifying and addressing IT security risks associated with that IT asset (Hardy, 2012). In the current era, organisations are still faced with the issue of understanding what threats to their IT assets are, their state of security, and how to obtain the necessary means to combat them (Mougouei, et al., 2012). The effects of

various threats vary considerably, ranging from small losses to entire IT system destruction and may affect the security posture of an IT asset. Underestimation of IT security risk from smaller scale security incidents often result in significant losses because many such vulnerabilities are not proactively detected, thus allowing IT assets to be attacked and damaged (Burns, 2005; Jouini, et al., 2014).

Knowing that a problem exists does not guarantee protection if appropriate action is not taken (Hardy, 2012). It is imperative for both individuals and organisations to be able to act correctly and in time to keep up with evolving threats in order to mitigate the associated risks. Researchers investigating IT security have proposed various theories and approaches for managing IT security threats which include modelling IT security threats (Jouini, et al., 2014).

A threat modelling process enables organisations to understand the complexity of an IT asset and identify possible vulnerabilities to that asset, regardless of whether or not those vulnerabilities can be exploited (Myagmar, et al., 2005). Threat modelling is used to discover the motives and techniques that an attacker would use to exploit vulnerabilities of an IT asset. A threat model should evolve because security threats evolve, as IT assets are rarely static and need to be adapted to suit changing business requirements (Meier, et al., 2003). Threat modelling should be an iterative process and continue throughout an IT asset's life cycle.

Having a document that identifies both the known threats and how they have been addressed (or not) puts an organisation in control of the security of an IT asset (Swiderski & Snyder, 2004). During the development of security requirements, threats should be analysed based on their criticality and likelihood, and a decision should be made on whether to mitigate the threat or accept the risk associated with it (Mougouei, et al., 2012).

One of the biggest mistakes that organisations often make is to skip the threat modelling process and simply extract IT security requirements and controls from industry's best practice frameworks (Myagmar, et al., 2005). However, industry best practice frameworks and standards only provide general IT security guidance and cannot address all of the distinctions of a particular IT asset. The threat modelling

process goes further by customising the target IT asset, defining additional requirements and, moreover, compiles a list of potential threats (Mougouei, et al., 2012).

Swiderski and Snyder (2004) and Burns (2005) emphasise that threat modelling should be a systematic process and cannot be conducted by simply brainstorming attackers' possible intentions. A good threat model should provide organisations with a basis to accurately estimate the attacker's capabilities and not leave large portions of the solutions' attack spaces not investigated (Jouini, et al., 2014).

Employing an adequate threat modelling process provides the following benefits:

- identification of potential threats and vulnerabilities depicting threat scenarios for an IT system that may assist to anticipate possible attacks (Swiderski & Snyder, 2004);
- justification of IT security features for IT assets where vulnerabilities are revealed for identified threats (Burns, 2005);
- development of a credible security classification model through a logical thought process in defining the security features of an IT system (Myagmar, et al., 2005); and
- verification of IT security features and increased resilience within the IT systems (Swiderski & Snyder, 2004).

Various threat modelling processes were investigated during this literature review, including the Microsoft application threat modelling process (Meier, et al., 2003), the SANS Institute application threat modelling process (Burns, 2005), Open Web Application Security Project (OWASP) Application threat modelling process (OWASP, 2015), and the National Center for Supercomputing Applications (NSCA) threat modelling process defined by Myagmar, et al. (2005). Table 4.1 provides a high-level analysis of the different threat modelling processes investigated in this study.

Table 4.1 – Threat Modelling Processes

	Microsoft Threat Modelling Process	SANS Threat Modelling Process	OWASP Threat Modelling Process	NCSA Threat Modelling Process
High-level Process	**1. Identify assets** • Identify the valuable assets that must be protected **2. Create an architecture overview** • Use simple diagrams and tables to document the architecture of the system including subsystems, trust boundaries, and data flows **3. Decompose the system** • Decompose the architecture of the asset including the underlying network and host infrastructure design • Create a security profile for the application to uncover vulnerabilities in the design, implementation, or deployment configuration of the asset **4. Identify the threats** • Keeping the goals of an attacker in mind, and with knowledge of the architecture and potential vulnerabilities, identify the threats that could affect the assets **5. Document the threats** • Document each threat using a common threat template that defines a core set of attributes to capture for each threat **6. Rate the threats** • Rate the threats to prioritise and address the most significant threats first	**1. View the system as an adversary** • Identify entry and exit points • Identify the assets • Identify the trust levels **2. Characterise the system** • Define use scenarios • Identify external dependencies • Identify external security controls • Identify internal security controls • Define implementation assumptions **3. Determine the threats** • Identify the threats • Classify the threats • Analyse the threats • Document the threats	**1. Decompose the application** • Identify assets • Gain an understanding of the assets and how they interact with external entities • Define use cases • Identify entry points to the assets • Identify trust levels • Document data flow diagrams for the asset • Document the threats **2. Determine and rank threats** • Categorise the threats • Define use and abuse cases • Determine the security risk for each threat **3. Determine countermeasures and mitigation** • Rank the threats • Document threat-countermeasure mapping lists • Document the threats and countermeasures to be implemented	**1. Characterise the system** • Define characteristics of the system • Define usage scenarios • Identify assumptions • Identify dependencies **2. Identify assets and access points** • Define the assets • Identify potential adversaries • Define the adversaries' motivations and goals • Define the information available to the adversaries that may be used to exploit the vulnerabilities • Identify access points to the systems • Define trust levels and boundaries **3. Identify threats** • Use the information gathered in the previous steps to identify internal and external threats **4. Specify security requirements** • Document the threats • Use a risk management process to prioritise threats • Specify security requirements for each system or asset

The SANS threat modelling process developed by Burns (2005) at a high level involves the following: viewing the system as an adversary (i.e. activities such as the identification of entry or exit points, identification of assets, and identification of trust level); characterising the system (i.e. activities such as defining use case scenarios, defining external dependencies, and modelling the system); and then developing a threat profile (i.e. defining security requirements).

The OWASP threat modelling process follows a similar process of decomposing the application, determining and ranking threats, and determining countermeasures for the identified threats (OWASP, 2015). The threat modelling process defined by Myagmar, et al. (2005) involves characterising the system, identifying assets and access points, identifying threats, and specifying security requirements.

The analysis revealed a common theme amongst the different threat modelling processes with variations at a granular level. An interesting point to note is that both the SANS threat modelling process defined by Burns (2005) and the OWASP threat modelling process make use of the threat modelling process defined by Meier, et al. (2003). Given these findings, the Microsoft threat modelling process defined by Meier, et al. (2003) is presented in detail, as it resonates all the other threat modelling processes analysed for this study. Figure 4.2 presents a basic six-step Microsoft threat modelling process developed by Meier, et al. (2003).

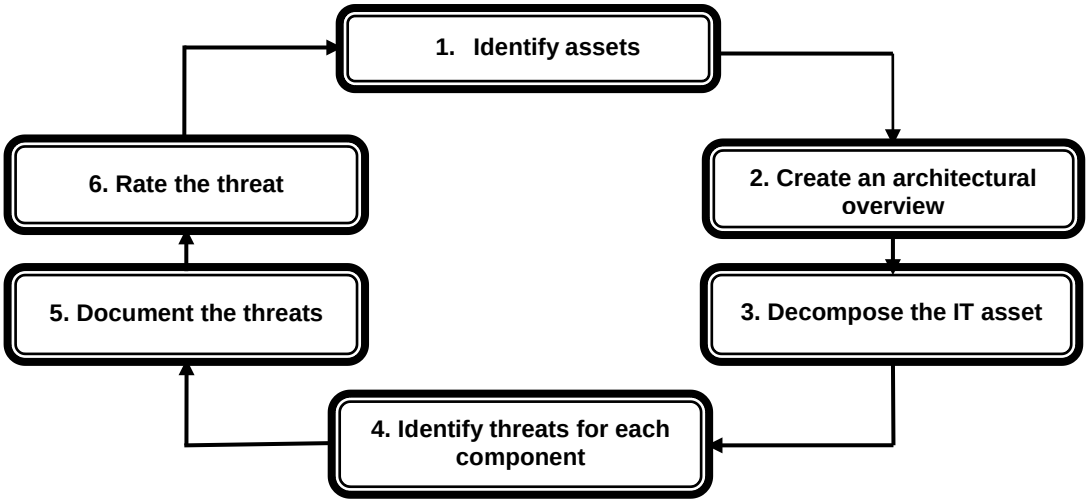

Figure 4.2 – The Microsoft Threat Modelling Process

Source: Meier, et al. (2003)

4.2.1. Step 1: Identify assets

The first step in the threat modelling process is to identify the assets that need to be protected (Meier, et al., 2003). Identifying assets will clarify which assets are important and why they should be protected (Burns, 2005). Assets that need to be protected may be, for example, hardware, customers' transactional data, and employee salary information (Myagmar, et al., 2005).

The different security principles that need to be protected for each asset should be defined (Meier, et al., 2003). For instance, the integrity of a financial process may be extremely important in one case, whereas confidentiality of employees' salary information may also be extremely important in another case.

4.2.2. Step 2: Create an architectural overview

The goal of this step is to document the function of the solution, its architecture, the software components, as well as the hardware components that form part of the entire solution, thus the IT asset (Meier, et al., 2003). Simple diagrams and tables that depict subsystems trust boundaries and data flows should be documented (Meier, et al., 2003). At this point, potential vulnerabilities in the design of the IT asset should be examined (Burns, 2005). The tasks performed include identifying what the IT asset does, creating an architectural diagram, and identifying technologies used to enable the functioning of the IT asset (Myagmar, et al., 2005).

The task of identifying what the IT asset does includes defining how the solution interfaces with other IT assets (Myagmar, et al., 2005). The various functions performed by the IT asset should be documented in order to set the functionality in context as well as help see how that IT asset can be misused or abused (Burns, 2005). The task of creating a high-level architecture diagram involves documenting the composition and structure of the IT asset, including subsystems and the physical deployment characteristics (Myagmar, et al., 2005). Different architectural models (i.e. conceptual, logical, physical, data, and business) of the solution should be documented, as they will describe the solution from different perspectives (Myagmar, et al., 2005). The last task in this step is to identify the technologies that will be used to implement the IT asset

such as an operating system in the case that an IT application is the IT asset (Myagmar, et al., 2005).

4.2.3. Step 3: Decompose the IT asset

This step involves creating a security profile for the IT asset (Meier, et al., 2003). The function of a security profile is to discover vulnerabilities in the design, implementation, or deployment configuration of the IT asset (Burns, 2005). Table 4.2 is an example of an IT asset that is decomposed.

Table 4.2 – Example of a Decomposed Solution

Application Decomposition		
Security Profile		Trust Boundaries
Input Validation	Session Management	Data Flow
Authentication	Cryptography	Entry Points
Authorisation	Parameter Manipulation	Privileged Code
Configuration Management	Exception Management	
Sensitive Data	Auditing and Logging	

Source: Meier, et al. (2003)

The idea behind this step is to identify and document various aspects of the IT asset. These aspects include trust boundaries, data flows, entry points, privileged code, and the security profile (Myagmar, et al., 2005).

The task of creating trust boundaries refers to analysing each tangible asset of the IT asset and considering whether data flow and user input are trusted to and from interfacing systems (Meier, et al., 2003). For example, if data flow and/or user input is not trusted between subsystems, then authentication and authorisation should be considered (Myagmar, et al., 2005). This task will ensure that all appropriate gatekeepers are in place, that they guard all entry points to individual trust boundaries, and that they validate all data passed to specific recipients across trust boundaries (Burns, 2005).

The second task in decomposing the solution is to identify and create data flows for the IT asset (Meier, et al., 2003). Creating data flows should follow a top-down approach, starting at the highest level and then iteratively decomposing the IT asset by analysing

the data flow between the subsystems (Myagmar, et al., 2005). It is advisable to use data flow diagrams as well as sequence diagrams to illustrate the formal decomposition of the system (Burns, 2005; Myagmar, et al., 2005).

The third task in this step involves identifying and analysing all entry points to the IT asset and subsystems. This is because they will also serve as entry points for attacks (Meier, et al., 2003).

The fourth task is to identify privileged code or resources that exist within the IT asset (Burns, 2005). Privileged code has the highest level of access which might severely compromise the IT asset if an attacker were to gain access to it (Myagmar, et al., 2005).

The last step in the task of decomposing the IT asset is to create the security profile for that particular asset (Meier, et al., 2003). Creating a security profile includes identifying the design and implementation approaches which are used for input validation, authentication, authorisation, and all other remaining areas where the solution might be susceptible to vulnerabilities (Burns, 2005).

4.2.4. Step 4: Identify threats for each component of the IT asset

To identify threats for each component of the IT asset, Meier, et al. (2003) suggests workshopping the different components with different subject matter experts. The idea behind this step is to ensure that potential scenarios of an attacker are kept in mind (Myagmar, et al., 2008).

Additionally, the use of attack trees and attack patterns (as depicted in Figure 4.3 and Table 4.3 respectively) is recommended because it assist in identifying other potential threats which may not have been considered (Meier, et al., 2003).

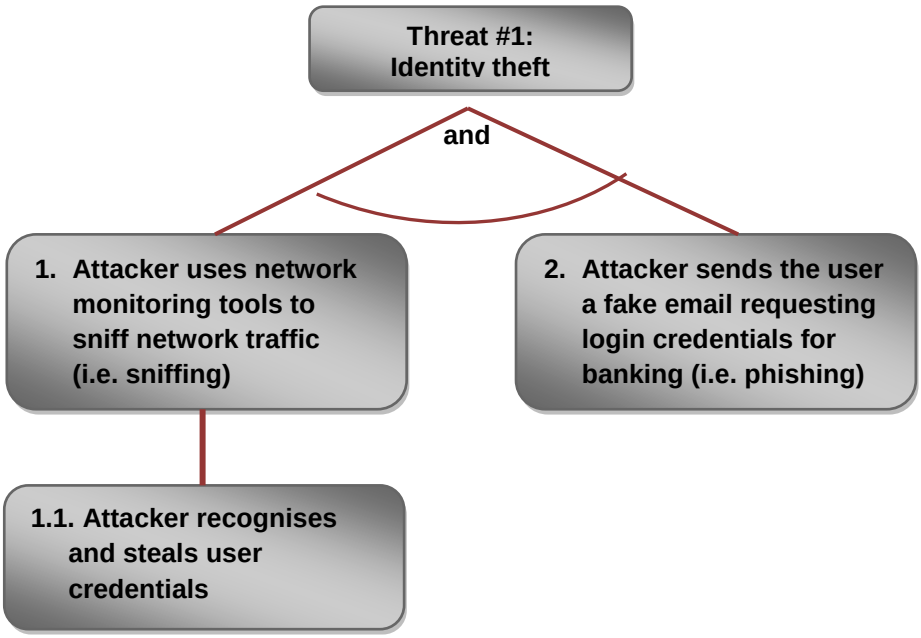

Figure 4.3 – Example of Using an Attack Tree

Source: Meier, et al. (2003)

Table 4.3 – Example using an Attack Pattern for Code Injection

Pattern	Code injection attacks
Attack goals	Command or code execution
Required conditions	*Weak input validation* Code from the attacker has sufficient privileges on the server.
Attack technique	1. Identify program on target system with an input validation vulnerability. 2. Create code to inject and run using the security context of the target application. 3. Construct input value to insert code into the address space of the target application and force a stack corruption that causes application execution to jump to the injected code.
Attack results	Code from the attacker runs and performs malicious action.

Source: Meier, et al. (2003)

The use of attack trees and attack patterns assists in probing one's thinking while conducting this exercise because a question is asked after each step (Meier, et al., 2003).

4.2.5. Step 5: Document the threats

For documenting threats, Myagmar, et al. (2005) recommends that a common threat template which defines the core set of attributes should be used. The threat capturing template should capture information for each IT asset, including such information as threat description, threat target, attack techniques, vulnerabilities exploited, and countermeasures required to address the threat (Meier, et al., 2003). As previously stated, threats evolve; on that account, documenting threats should also be an iterative process (Burns, 2005).

4.2.6. Step 6: Rate the threats

This step involves rating the threats in order to prioritise and address the most significant threats first (Meier, et al., 2003). Both quantitative (e.g. *risk = probability * damage potential*) and qualitative (e.g. *high, medium, low*) approaches can be used to rate the threats; the decision depends on the preference of an organisation (Myagmar, et al., 2005).

Furthermore, a systematic process or an ad hoc process can be applied for rating the IT security threats (Burns, 2005). The use of ad hoc methods for rating threats has proven to be more subjective because the attributes used to rate the threats are not predefined and may differ with every audience that performs the threat rating (Meier, et al., 2003). Therefore, for the purpose of this study, a systematic method is used.

The Microsoft, NSCA and OWASP threat modelling processes all use the Microsoft DREAD as a threat rating method. Microsoft DREAD is a structured method which is a hybrid of qualitative and quantitative approaches (Meier, et al., 2003). The rating process for Microsoft DREAD weighs the probability of the threat against the damage that could result should an attack occur (Meier, et al., 2003). It might turn out that certain threats do not warrant any action when you compare the risk posed by the

threat with the resulting mitigation costs (Myagmar, et al., 2005). Table 4.4 presents an example of the Microsoft DREAD rating table.

Table 4.4 – Example of a Threat Rating Table using DREAD

-	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorisation; run as administrator; upload content.	Leaking sensitive information.	Leaking trivial information.
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack and then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers.	Some users, non-default configuration.	Very small percentage of users; obscure feature; affects anonymous users.
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Source: Meier, et al. (2003)

The Microsoft DREAD is used to rate the threats systematically using the five basic attributes defined as follows (Meier, et al., 2003):

Damage potential: How significant is the damage if the vulnerability is exploited?
Reproducibility: How effortless is it to reproduce the attack?
Exploitability: How easy is it to launch an attack?
Affected users: As a rough percentage, how many users are affected?
Discoverability: How easy is it to find the vulnerability?

Once the threat rating table has been defined and agreed, threats are rated by aggregating the DREAD attributes and comparing the totals for the different threats, as depicted in Table 4.5.

Table 4.5 – Microsoft DREAD Rating Example

Threat	D	R	E	A	D	Total	Rating
Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
SQL commands injected into application.	3	3	3	3	2	14	High

Source: Meier, et al. (2003)

As previously stated, the output of the threat modelling process is documentation of the security features of an IT asset which includes a list of rated threats (Burns, 2005). The next section discusses the classification of threats, another important aspect of threat modelling (Myagmar, et al., 2005).

4.3. CLASSIFICATION OF THREATS

IT security threats have increased exponentially in recent years because there are different types of IT security threats emerging on a frequent basis which are more complex (Burns, 2005). Threat modelling can be supported by threat libraries which are found particularly effective and defined by different organisations in the discipline of security (Uzunov & Fernandez, 2013).

Even though threat libraries offer much value, they only encompass a set of specific, predefined threats, making the discovery of new threats or the same threats in different architectural contexts more difficult (Myagmar, et al., 2005). For that reason, a structured approach would potentially provide various benefits such as allowing an arbitrary number of threats to be categorised (Meier, et al., 2003). Various authors (Amoroso, 1994; Lindqvist & Jonsson, 1997; Jouini, et al., 2014) concur that a robust IT security threat classification process should be guided by principles which are used to evaluate threat classifications.

The common principles extracted by Jouini, et al. (2014) from various studies are presented as follows:

- **Mutually exclusive:** Threat categories should not overlap. Every threat that is classified in one category should exclude all other categories, thus only fit in, at most, in one category.
- **Exhaustive:** The threat classification categories should include as many threat specimens as possible to ensure that all threats are catered for.
- **Unambiguous:** Threat categories should be consistent, clear and precise to ensure that during the process of classifying threats, they are as certain as possible.
- **Repeatable:** When a threat classification is performed on one IT asset by different individuals, it should result in the same classification.
- **Accepted:** Threat categories should be logical, native and easily acceptable by the majority.
- **Useful:** Threat classifications should provide the user with more insight into the field of inquiry and also be easily adaptable to different application needs.

There are various threat classification models which can be used in the threat classification process (Alhabeeb, et al., 2010). Some threat classification models are more general and less detailed than others based on whether the organisation is more stable or not (Alhabeeb, et al., 2010). The simplest way to apply the threat classification process is to examine components of the IT asset, consider how each of the threats affects each component, and then record all the threats within the specific categories (Jouini, et al., 2014).

It is important to note that there are many threat modelling methods developed by various authors in the current body of knowledge under the IT security discipline. For the purpose of this study, the threat classification models discussed are Microsoft STRIDE, National Institute of Standards and Technology (NIST) classification, Computer Security Institute (CSI) classification, and the International Standards

Organisation/International Electrotechnical Commission (ISO/IEC) 17799:2000 classification.

4.3.1. Microsoft STRIDE

Microsoft STRIDE is a threat classification model which uses threat or attack taxonomies to classify IT security threats (Burns, 2005). STRIDE is an acronym for **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service and **E**levation of privileges (Meier, et al., 2003).

Spoofing refers to when adversaries deceive applications or users by using authentication information (e.g. username and password) which does not belong to them in order to gain access to IT systems or applications which they are not authorised to have (Myagmar, et al., 2005). Tampering refers to the malicious modification of information by unauthorised parties (Meier, et al., 2003). Repudiation refers to threats whereby users or adversaries deny taking accountability for the actions that they have performed and there is lack of ability for the system to produce proof (Jouini, et al. 2014). Information disclosure refers to threats that have the objective of exposing information to unauthorised parties (Fenz & Ekelhart, 2009).

Denial of service threats are threats which attack IT systems by denying services provided to authorised users, thereby making the IT system unavailable for a specific period (Krichene, 2008). Elevation of privileges refers to threats whereby adversaries gain unauthorised privileged access and then use it to perform malicious activities (e.g. penetrating and deleting all system defences) (Klemen & Biffl, 2004).

4.3.2. National Institute of Standards and Technology (NIST) classification

The NIST classification threat classification model was initially designed with the objective of ensuring that threats categories are not repeated over the different departments (NIST, 2004). There are six threat categories: errors and omissions; fraud and theft; employee sabotage; loss of infrastructure that supports the system; malicious hackers; and malicious code (NIST, 2004).

Errors and omissions refer to threats that affect data and system integrity as a result of internal system users making unintentional mistakes (Ajibuwa, 2008). Fraud and theft

refer to threats to IT systems that are due to traditional fraud and theft committed by people (e.g. employee using an IT application to steal small monies from different accounts of customers which amounts to a large sum) (Felegyhazi, 2011).

Employee sabotage refers to threats which arise from employees' deliberate, malicious actions (e.g. destroying hardware or facilities, and crashing systems intentionally) (Finne, 1996). Loss of infrastructure that supports the system is a threat which would typically result in system downtime, which is beyond the control of the system owners (e.g. fire, flood, and power failures) (Foley, 2009).

Malicious hackers are adversaries who attempt to break down the security defences of IT systems of a target organisation which often results in unstable IT systems, stolen data, and modified data (NIST, 2004). Malicious code includes all threats which come in a form of software and then attempts to perform some kind of malicious actions on the IT systems (Krichene, 2008). Examples of malicious code include viruses, Trojan horses, worms, logic bombs, and backdoors (NIST, 2004).

4.3.3. Computer Security Institute (CSI) classification

The CSI classification was initially developed by CSI as a result of a survey which was conducted in 2008 and which focused on computer crime and security (Alhabeeb, et al., 2010). The survey has since been conducted on an annual basis, and the target audience is security specialists who are urged to provide insight to current and new threats (Alhabeeb, et al., 2010).

The threats are classified into denial of service type threats (including laptop theft, telecom fraud, unauthorised access, virus, financial fraud, insider abuse, system penetration, and sabotage) and all other threats (including abuse of wireless network, website defacement, misuse of Web application, bots, DNS attacks, instant messaging abuse, password sniffing, and theft/loss of customer data from mobile devices) (Alhabeeb, et al., 2010).

4.3.4. ISO/IEC 27005 classification

The ISO/IEC 27005 threat classification categorises threats based on the sources of threats (Geric & Hutinski, 2007). The threats are grouped at a high level as follows (Geric & Hutinski, 2007):

- **Natural sources:** fire, earthquake, flood, incidents, storm, and pollution
- **Technical sources:** communication errors, technical mistakes, malfunctions, and radiation
- **Un-attention people sources:** indiscipline, negligence, unsuitable software, and unsuitable organisations
- **Attention people sources:** destruction, sabotage, diversion, war destruction, viruses, fraud, and stealing

4.4. CONCLUSION

This chapter presented a threat modelling process from Microsoft, which is high level and generic. The objective was to provide a basic understanding of how threat modelling can be applied within organisations. The threat classification models used globally by different organisations were discussed. These threat classification models include Microsoft STRIDE, NIST classification, CSI classification and the ISO 27005 classification. Even though the threat classification models were different in the categories, there were many similarities when it comes to the actual threats.

Having reviewed the basic risk management principles as well as the IT security frameworks and standards in Chapter 3 and the threat modelling process, there is sufficient theoretical foundation to define the ITSRB approach. The following chapter discusses the ITSRB approach.

5. THE INFORMATION TECHNOLOGY SECURITY RISK BASED (ITSRB) APPROACH

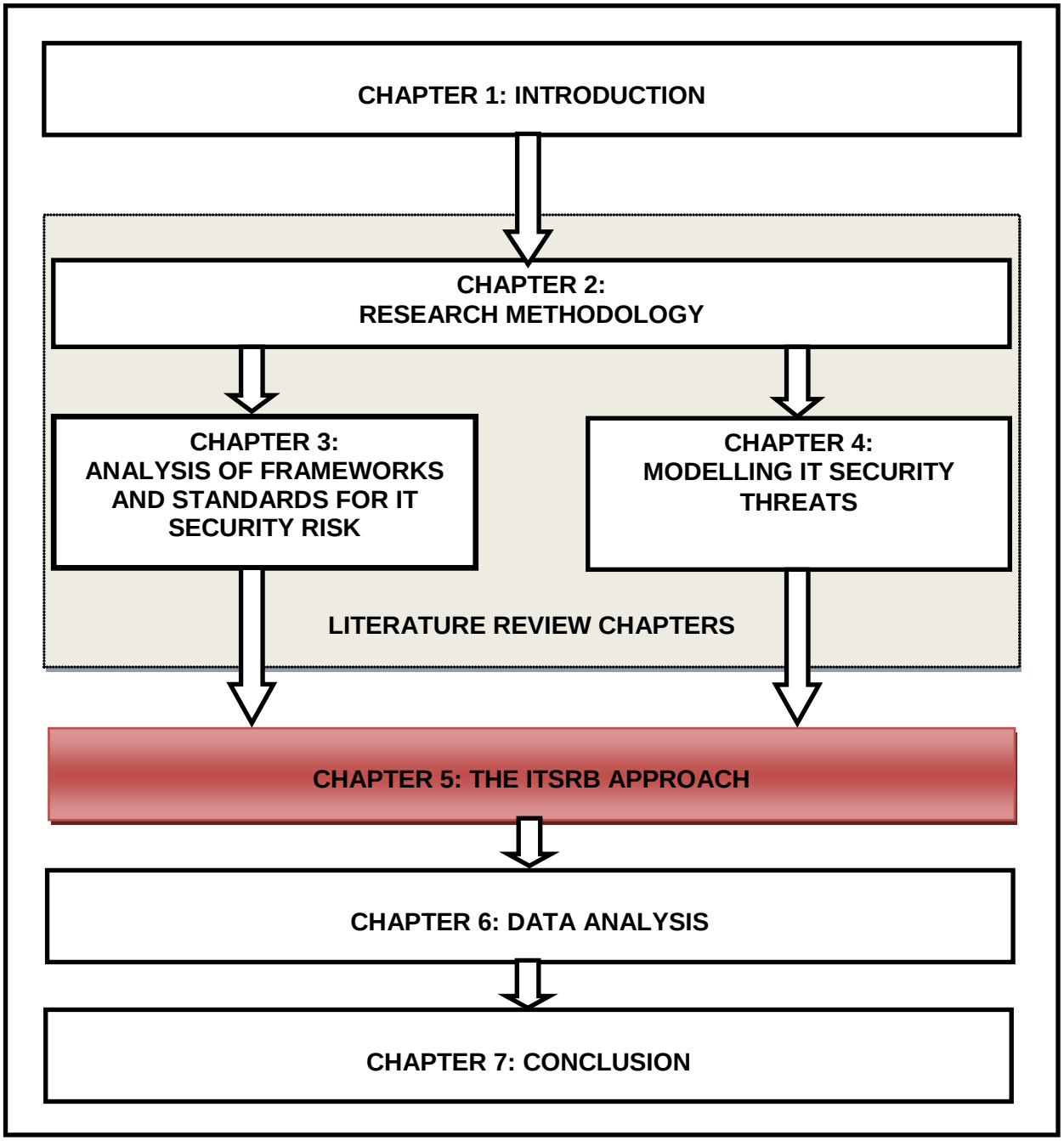

Figure 5.1 – Dissertation Layout: Chapter 5

5.1. INTRODUCTION

The previous chapter dealt with modelling IT security threats. The objective of this chapter is to propose an approach to identifying, assessing and treating IT security risk which incorporates a robust risk analysis and assessment process. The proposed IT Security Risk Based (ITSRB) approach uses coherent characteristics of the risk management principles and IT security frameworks and standards discussed in Chapter 3. Additionally, the threat modelling process discussed in Chapter 4 is also used to enhance the ITSRB approach.

To ensure that the ITSRB approach integrates all the necessary elements to enable it to be more effective when it is applied in a real-world situation, Zachman (2011) recommends the Kipling method (i.e. asking the what, why, who, how, when and where questions). The use of the Kipling method in defining a framework helps to explore the problem by probing the thinking of the problem-solver with the questions: what, why, how, who, when and where (Sherwood, et al., 2009). In the same vein, the Kipling method was applied to explain the ITSRB approach.

What: The ITSRB approach is a proactive and dynamic method that aims to ensure that IT security risk is effectively and holistically managed. In principle, the ITSRB anticipates reducing the risks associated with security of IT assets.

Why: The motivation behind defining the ITSRB approach is to formulate a method to assist in managing IT security risk, thereby guaranteeing that relevant risk is addressed with adequate and effective controls at the right time.

How: The ITSRB approach uses a combination of best practice IT security risk management frameworks and standards as well as a threat modelling process to ensure that risk emanating from both known and unknown threats in the IT environment is managed.

When: A pragmatic tactic is used when applying the ITSRB approach in order for it to add value. Using a pragmatic tactic to manage IT security risk ensures that the ITSRB approach is guided by the nature of the risk that each organisation faces.

Where: The ITSRB approach is applied within the IT environment of an organisation.

Who: IT security professionals within any organisation can use the ITSRB approach.

This chapter is divided into four sections. Section 5.2 presents a comparative analysis of the IT security frameworks and standards discussed in Chapter 3 in a summarised manner. Section 5.3 shows the attributes of a good IT security risk management approach deduced from Section 5.2. Section 5.4 brings forward the proposed ITSRB approach. Section 5.5 concludes the chapter.

5.2. COMPARATIVE ANALYSIS OF THE SELECTED BEST PRACTICE IT SECURITY FRAMEWORKS AND STANDARDS

The various frameworks and standards discussed in Chapter 3 have similar objectives with regard to IT security. These are to safeguard the confidentiality, integrity and availability of information and/or systems. The primary differences lie in the approach followed in managing IT security risk (Ajibuwa, 2008; Saleh & Alfantookh, 2011).

Cheney and Furner (2008) discuss four categories of frameworks which the investigated IT security frameworks and standards may fall into, namely, strategic, technical, compliance, and high-level guidelines. COBIT 5 is an IT governance framework with security governance as a sub-component. COBIT 5 focuses on ‘what’ must be done rather than ‘how’ it must be done and is strong in providing high-level integration required in the cohesion of various IT security programmes (Cheney & Furner, 2008). Similarly, ITIL is an IT governance framework with security management as a sub-component. ITIL, on the other hand, is more technically orientated in nature, focusing on ‘how’ things should be done rather than ‘what’ should be in place (Cheney & Furner, 2008).

Table 5.1 provides a summarised view of the five selected IT security frameworks and standards discussed in Chapter 3. As previously indicated, there are many IT security frameworks and standards found in the current body of knowledge. The reason the five frameworks and standards were selected and discussed in detail in this study is because they are commonly used within South African financial institutions, which falls within the scope of this study.

Table 5.1 – Summarised View of the IT Security Frameworks and Standards

	OCTAVE	ISO 27001	COBIT	ITIL	ISF
Focus	IT and information security risk	Information security for both IT and business	IT governance	IT service management	Information security and information risk
Applicability Level	Strategic	Tactical	Strategic	Tactical	Tactical
Characteristics	• Organisational focus • Risk based: balances operational risk, security practices and technology • Seeks accountability for assets, threats, vulnerability and impact • Consists of three phases: Build Asset-Based Threat Profiles, Identify Infrastructure Vulnerabilities, and Develop Security Strategy and Plans	• Provides guidance to organisations on how to implement security controls • Used as a model to build an ISMS • Holistic risk based view while enabling benefits from business opportunities • Based on Plan-Do-Check-Act cycle • Consists of detailed 133 security measures which are organised into 11 domains and 39 control objectives	• Best practice processes for IT domains defined by group of experts within various areas of IT • Grouped in five focus areas which summarise its activities (i.e. strategic alignment, value delivery, resource management, risk management, and performance measurement) • Consists of four core domains related to planning, building, running, and monitoring of the IT environment • Applies to all IT resources, namely, Applications, Information, Infrastructure, and People	• Primary objective is to provide an organisation with good quality information collection, information analysis, information production, and information distribution • IT services recognised as crucial and strategic assets invested in which should be measured and improved • Consists of four life cycle stages: service strategy, service design, service transition, and service operations with continual service improvement existing throughout the life cycle	• Defined and created by information security experts around the world, in a way that enables compliance with other recognised frameworks (e.g. ISO 27001 and COBIT) • Provides a basis for a detailed or a high-level organisational information security assessment • Divided into four categories: security governance, security requirements, control framework, and security monitoring and improvement

	OCTAVE	ISO 27001	COBIT	ITIL	ISF
Key Strengths	• Systematic and context-driven • Self-directed • Workshop-based approach • Involves junior staff up to senior/executive management	• Globally recognised, enabling enterprises to use it as an assurance tool or a benchmark tool • Can increase business and IT alignment • Can enable organisations to measure which security controls provide the largest return on security investment • Improved effectiveness of information security because of the use of tried-and-tested best practice guidance • More technically detailed, and therefore provides comprehensive guidance on how things should be done	• Can increase business and IT alignment • Organises IT activities into a generally accepted process model • Enables the organisation to see major IT resources to be leveraged • Defines the management control objectives to be considered	• Can increase user and customer satisfaction because IT services are explicitly defined and service levels are measured • Improved decision-making and optimised risk because all aspects relating to every IT service are taken into account during design, analysis and operation • Can offer financial savings from reduced rework, lost time, improved resource management and usage • Service catalogue is explicitly defined; therefore, there is improved time to market new IT products and services • Can improve IT service availability because IT service levels are closely monitored	• Rigour and comprehensive, allowing for a more effective process of key risks identification • Provides a detailed set of controls which covers the IT environment holistically, hence minimising the need to purchase additional repository of potential controls • Seamless integration into an organisation because it is completely aligned with other globally recognised security frameworks

	OCTAVE	ISO 27001	COBIT	ITIL	ISF
Weaknesses	• Resource intense: requires human time investment and formal training in some cases • Focus is mainly on identification, analysis and planning, and no focus on implementation, monitoring and control activities • Dedication of top management is often a challenge • Assessment of a complex organisation might consume much time, resulting in misinterpretation of the information gathered due to changes happening during the exercise	• Scope of implementation is considerably large, therefore cannot be implemented all at once • Limited expertise within organisations' resources makes it difficult to envisage what the end result should be • Resistance to change from employee behaviour might be a challenge • Associate cost and effort of implementation may be lengthy and become a big factor	• High degree of abstraction • Poor focus on IT, bringing unrelated practices under one umbrella, which makes it weak to some of the core services that IT offers • It is thin on detail regarding 'how things should be done' • Not an exclusive information security standard; therefore, COBIT cannot be relied upon for the entire security program within an organisation	• Failure to fully understand the breadth and depth of ITIL may lead to implementation failures • Has a high level of detail which becomes a challenge for senior management (especially those with no IT background) to fully understand and support • All ITIL-aligned processes and performance aspects require roles or individuals to be assigned to them, which is often a daunting task for many organisations • Day-to-day operations can become more about the processes than service delivery, thus failing to deliver to the business • Limited in the area of IT, and security not a core focus	• Dependent on the use of frameworks and yields most value when it is used as a supporting framework and not as a stand-alone framework • Might introduce too much ambiguity because it leaves the users with too much room for flexibility with regard to interpreting how controls should be implemented • Compliance-focused and not effectiveness-focused; it does not help if an organisation is considered compliant because controls exist but those controls are not working effectively to address day-to-day operational challenges

5.3. ATTRIBUTES OF A GOOD IT SECURITY RISK MANAGEMENT APPROACH

The five attributes which have been observed as making up a comprehensive and more effective IT security risk management approach are discussed in this section. These attributes have been derived through the detailed analysis of the risk management and IT security frameworks and standards discussed in Chapter 3. A comparative analysis of the investigated IT security frameworks and standards presented in Section 5.2 indicates that there are different approaches to managing IT security risk. Other frameworks and standards are applied at a strategic level, whereas others are focused at a tactical level. Additionally, some of those frameworks and standards focus on the 'what' while others focus on the 'how'. In finding a good approach to IT security risk management, strong characteristics from the investigated frameworks and standards are extracted to define the proposed ITSRB approach.

5.3.1. ATTRIBUTE 1: Hybrid approach

The first attribute essential for ensuring coverage of an organisation's IT security risk profile is a hybrid approach, depicted in Figure 5.2. To ensure that the entire IT security risk profile is covered, a combination of a top-down approach and a bottom-up approach, namely, a hybrid approach should be applied to identify and manage IT security risk (National Institute of Standards and Technology [NIST], 2010). NIST (2010) states that managing IT security risk requires the involvement of the entire organisation, from senior management to the most junior employee.

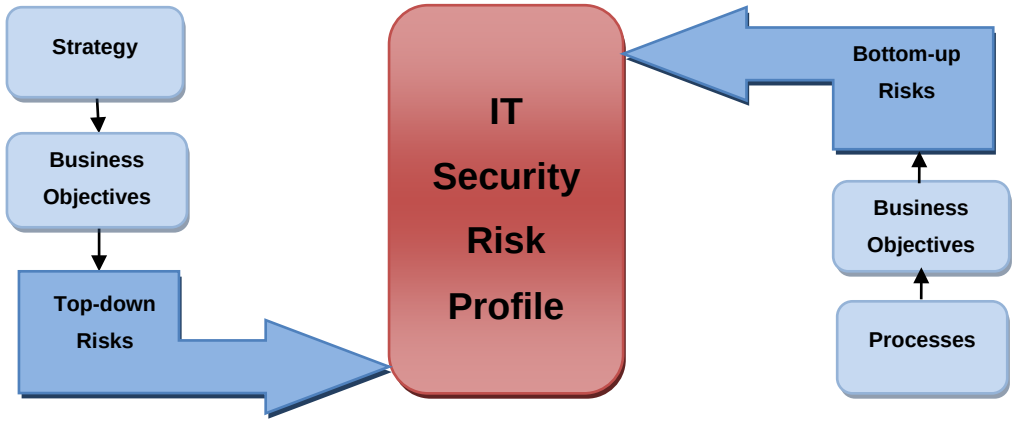

Figure 5.2 – The Hybrid Approach

The comparative analysis presented in Section 5.2 indicates that applying an IT security risk management framework only at a strategic level of an organisation may leave out other significant IT security risks found at tactical and operational levels of an organisation (NIST, 2010). Thus, it is advisable to take a more holistic approach.

Senior management is responsible for providing the strategic vision, goals and objectives of the organisation, while mid-level management is responsible for planning and managing projects as well as processes. On the other hand, junior staff are responsible for carrying out operational activities (NIST, 2010). Figure 5.3 depicts the tiered risk management approach recommended by NIST (2010).

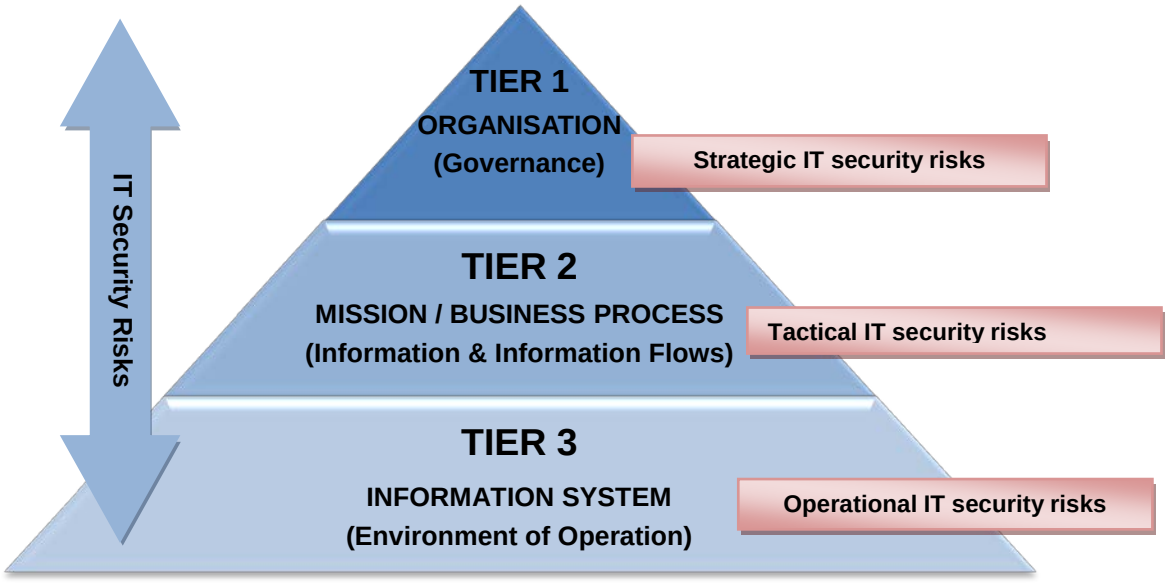

Figure 5.3 – Tiered Risk Management Approach

Source: NIST (2010**)**

In a tiered risk management approach, risks at tier 1 are strategic risks; at tier 2, they are tactical risks; and at tier 3, risks are operational risks (NIST, 2010). OCTAVE and COBIT 5 are applied at a strategic level by recommending the governance aspects of IT security. ISO 27001, ITIL and ISF are applied at tactical level by recommending the operational controls for IT security. The proposed ITSRB approach uses the hybrid approach. This is also indicated by the comparative analysis in Table 5.1.

5.3.2. ATTRIBUTE 2: Iteration

The Institute of Risk Management (IRM, 2010) emphasises that treatment of any kind of risk should be an iterative process, which is the second attribute essential for the proposed ITSRB approach. Therefore, an IT security risk management process should be an iterative process that is defined in a way that will lead to continuous improvement of an organisation's risk posture (Ketel, 2008). Application of this attribute is demonstrated in all of the frameworks and standards reviewed by the comparative analysis in Table 5.1. ISO 2700:2005, which is a standard recommending best practice operational controls for security, further puts a structure to the iteration attribute by introducing the Deming cycle. The Deming cycle is also known as the Plan-Do-Check-Act (PDCA) model and is depicted in Figure 5.4.

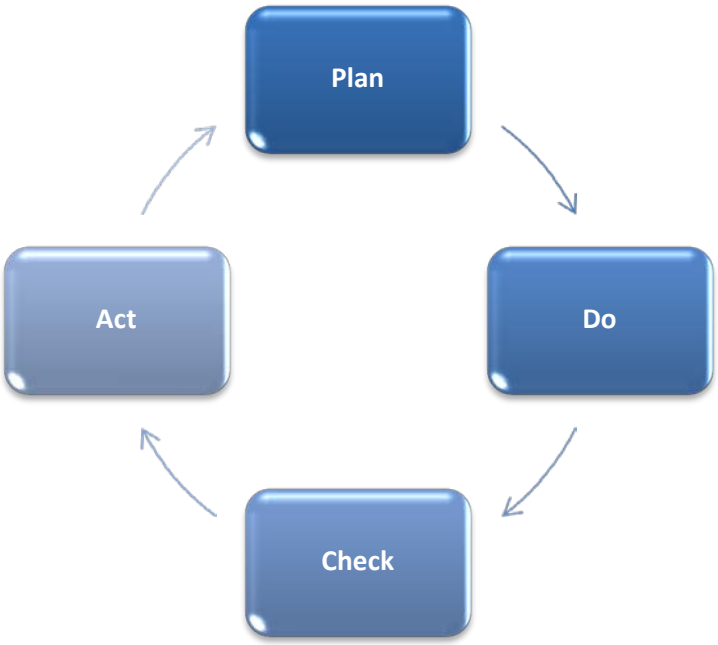

Figure 5.4 – PDCA Model

Source: (Averson, 2015)

The PDCA model recommends that IT security initiatives be planned, executed, monitored and maintained (ISO/IEC 27001, 2013). The model allows organisations to continuously self-assess themselves by engaging in improvement activities throughout the management of IT security risk (ISO/IEC 27001, 2013). For these reasons, the iteration attribute is applied in the proposed ITSRB approach.

5.3.3. ATTRIBUTE 3: Responsibility assignment

In identifying the responsibility of tasks for any process, the RACI (Responsible, Accountable, Consulted, and Informed) is an appropriate tool to be used (Smith & Erwin, 2005). The RACI model basically helps to simplify the responsibilities in a process by creating a two-dimensional matrix which shows the 'level of involvement' for functional roles in a set of activities, as demonstrated in Table 5.2 (Smith & Erwin, 2005; Banacorsi, 2011).

Table 5.2 – Example of a RACI model

Process Name	Role 1	Role 2	Role 3	Role 4
Process 1	R	A	C	I
Process 2	A	I	R	C
Process n	I	R	A	C

RACI is defined as follows:

R: Responsible refers to the individual(s) who own the problem, activity or process (Smith & Erwin, 2005). The responsible individual(s) execute that specific process (Banacorsi, 2011). Responsibility can be shared or delegated (Banacorsi, 2011).

A: Accountable refers to the individual who is liable (Smith & Erwin, 2005). The accountable individual(s) are responsible for approving the task before it can be used (Banacorsi, 2011). Accountability cannot be delegated or shared (Smith & Erwin, 2005).

C: Consulted refers to the individual(s) who have the information and/or ability necessary to complete the specific process (Banacorsi, 2011). This individual(s) should be consulted before a key decision is taken regarding the process or activity (Smith & Erwin, 2005).

I: Informed refers to the individual(s) that must be notified about the results once an action has been taken (Banacorsi, 2011). Informed individual(s) are notified because

the action(s) taken have some level of impact on their function (Smith & Erwin, 2005).

The RACI model helps sort out the fundamental issues within a process where there is ambiguity in ownership of tasks (Banacorsi, 2011). Effective usage of the RACI model in a process will explicitly identify ownership, reduce duplication of effort and reduce misunderstanding (Smith & Erwin, 2005; Banacorsi, 2011).

COBIT is the only framework out of the investigated frameworks and standards that recommends the use of a RACI model throughout its domains, as mentioned in Chapter 3. IT Governance Institute (ITGI) (2007) emphasises that understanding roles and responsibilities for each process is important and forms the basis for effective governance. For these reasons, the RACI model has been applied for the proposed ITSRB approach, as it is regarded as an important attribute for assigning ownership in the IT security risk management process.

5.3.4. ATTRIBUTE 4: Input and output

Both the ITIL and COBIT frameworks emphasise that a process is a set of executable step(s) which has the primary objective of transforming input to output in order to achieve a known goal (ITGI, 2007; IT Service Management Forum [ITSMF], 2007). Calder (2013) recommends that a key and basic principle that is applicable to any process is that it should have an input and output. It is important to note that any process is defined to achieve the one goal of transforming input to output (Calder, 2013). Figure 5.5 presents a simple process model.

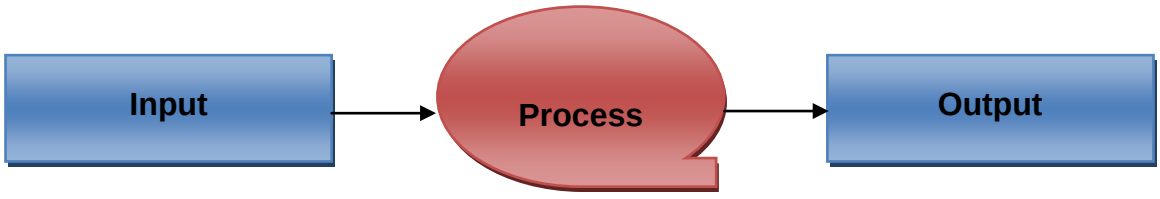

Figure 5.5 – A Simple Process Model

Calder (2013) emphasises that every input element put through a process should have some form of output as a product. A process is meant to transform input to output (Calder, 2013). The COBIT framework explicitly demonstrates the use of

inputs and outputs in all its processes, whereas OCTAVE, ITIL, ISO 27001 and ISF only emphasise the output components. For this reason, the proposed ITSRB approach uses this principle.

5.3.5. ATTRIBUTE 5: Dynamicity

Before defining the security controls of an IT system, it is essential to enumerate the threats to the system in question in order to help system architects or designers to develop realistic and meaningful security requirements (Myagmar, et al., 2005). Gandotra, et al. (2012) have demonstrated that it is important to implement a risk approach that is vigorous so that risk can be treated in a proactive manner. The integrated framework defined by Gandotra, et al. (2012) is defined in a way that ensures that both known and unknown threats can be identified and mitigated as they emanate or change.

Winter and Schelp (2008) have indicated that IT is dynamic, and for this reason, IT security threats also change quite often. Accordingly, in order to achieve this principle, it is important to define an approach that will periodically cater for the changing threats of the IT environment through a continuous monitoring exercise recommended by Hardy (2012).

The five attributes discussed above are elementary and sourced from various pieces of literature, but they are not all-inclusive enough to fully define the ITSRB approach proposed in this study. The next section presents the proposed ITSRB approach, which is based on the characteristics of the selected IT security frameworks and standards discussed in Chapter 3.

5.4. THE IT SECURITY RISK BASED (ITSRB) APPROACH

5.4.1. Structure of the ITSRB approach

It is common practice for frameworks to follow a structured life cycle, as highlighted by the comparative analysis in Section 5.2. Additionally, the “iteration” attribute as defined in Section 5.3 highlights the importance of using a systematic process that is continuous for IT security risk management. Furthermore, as previously stated in

Chapter 1, one of the objectives is to reuse the best characteristics of the best practice frameworks and standards in order to avoid reinventing the wheel. Accordingly, the ITSRB approach does not deviate from this practice and adopts the PDCA model as well as the iteration attribute to ensure its continuous improvement. Figure 5.6 presents the four phases of the proposed ITSRB approach based on the PDCA model which was adopted from the ISO 27001 framework.

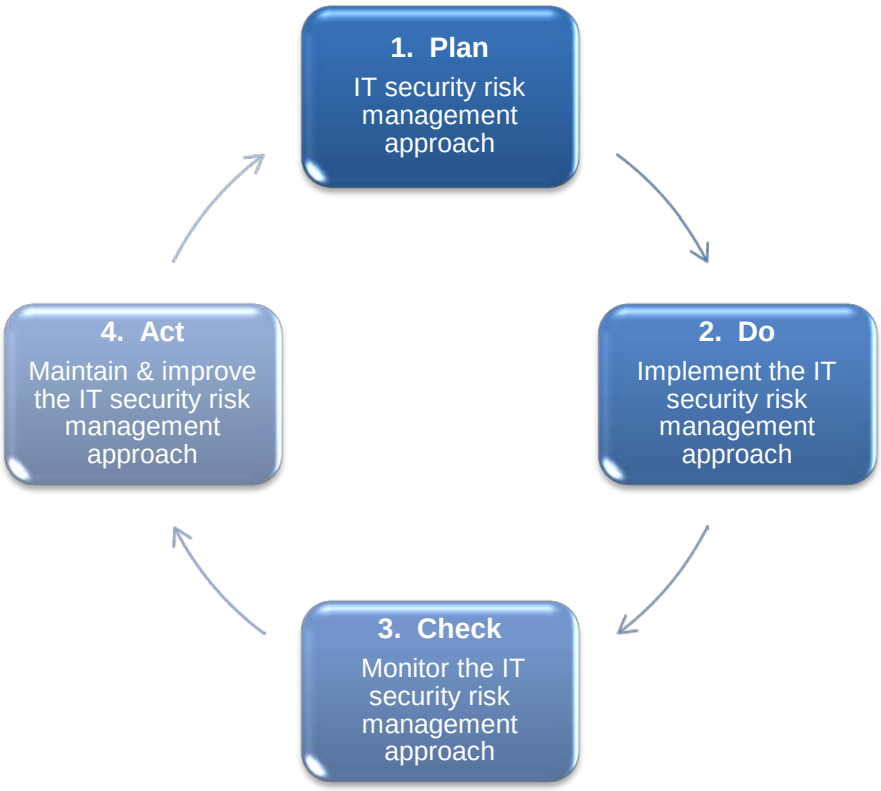

Figure 5.6 – Structure of the ITSRB Approach

Plan refers to establishing the proposed IT security risk management approach.

Do refers to the activities involved in implementing and operating the proposed IT security risk management approach.

Check refers to the process of monitoring and reviewing the IT security risk management approach.

Act refers to the process of maintaining and improving the IT security risk management approach which involves maintaining the IT security controls.

5.4.2. Features of the ITSRB approach

To clearly articulate the ITSRB approach, a number of features were defined to ensure that there is consistency in explaining each phase of this approach. The features selected align with the attributes discussed in Section 5.3. These features basically assist in grouping the characteristics that guide the ITSRB approach to make sure that a comprehensive view of this approach is explained in detail. Additionally, the features of the ITSRB approach are used to ensure that the target audience making use of this approach have an idea of exactly what will be required from them to manage IT security risk within their organisations.

The features of the ITSRB approach are defined as follows:

Phase: As per Figure 5.6, the ITSRB approach has four phases based on the PDCA model. This implies that it goes through different phases in order to achieve its goal. A phase basically refers to one of the sub-processes or stages of the ITSRB approach. This feature aligns with attribute 2 (i.e. iteration) described in Section 5.3.2.

Objective: Objective refers to the aim of each ITSRB approach's phases. The objective describes what each phase intends to do. Explaining the objective of each phase ensures that the users of the ITSRB approach comprehend the intention thereof.

Target audience: Target audience refers to the person(s) which each phase of the ITSRB approach is beset at. The different target audiences will be categorised according to their work responsibilities as per Figure 5.3, where tier 1 refers to people responsible for strategic management of an organisation; tier 2 refers to people performing tactical management duties within an organisation; and tier 3 refers to people performing operational management duties within an organisation. This feature aligns with attribute 1 (i.e. hybrid approach) described in Section 5.3.1.

Frequency: Frequency is the rate of occurrence that a specific phase should be conducted. The frequency that is specified in the ITSRB approach is the minimum frequency; therefore, any additional executions of phases will not cause any concerns. This feature aligns with attribute 5 (i.e. dynamicity) described in Section 5.3.5. This feature intends to promote consideration of various threats on a continuous basis.

Process model (i.e. input, process and output): The process model provides the input elements, the process that will be used to transform the input elements and the output elements. The basics of the process model align with attribute 4 (i.e. input and output) described in Section 5.3.4.

Tools: Tools refer to the existing frameworks, processes, applications or technologies that can be used in order to execute a process within a specific phase. Because organisations operate differently and use different applications, the ITSRB does not prescribe any specific application. Instead, the ITSRB approach emphasises the need to capture specific information as it best suits the users.

RACI: RACI is for responsibility assignment. RACI shows who will be responsible for what within each phase. The objective of this feature is to ensure that the users of the ITSRB approach understand their responsibilities within each phase. This feature aligns with attribute 3 (i.e. responsibility assignment) described in Section 5.3.3.

5.4.3. Phases of the ITSRB approach

The following tables present the phases of the ITSRB approach.

Table 5.3 – ITSRB Approach Phase 1

PHASE 1	**PLAN:** THE ITSRB APPROACH		
OBJECTIVE	The objective of this phase is to define and develop an IT security risk management plan that is fit for purpose for a specific organisation. The plan basically provides a view of what IT security controls are in the IT environment versus what IT security controls need to be in the IT environment (i.e. for software, hardware, procedures, networks, people and procedures).		
FREQUENCY	Annually		
TARGET AUDIENCE	• Strategic Management • Tactical Management		
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**
	• Organisational strategy (Objectives) • IT strategy • Previous IT security risk register (if it exists) • Previous IT audit report (i.e. IT security audits) • Previous IT security incidents	• Map each organisational strategy and IT strategy objective to an IT security principle (i.e. confidentiality, integrity and availability). • Define IT security requirements for each strategic objective and assess which IT security controls exist and which do not exist. • Use the COBIT control objectives to conduct a gap analysis to assess which controls exist within the IT environment and which ones do not exist. • Define the IT security risk appetite (i.e. this information should be sourced from the senior executive who is in charge of the IT environment, such as a chief information officer (CIO)).	• IT security strategy • IT security risk appetite • IT security risk profile • IT security risk register

PHASE 1	**PLAN:** THE ITSRB APPROACH			
		• The gaps identified from the strategic objectives as well as the gaps identified from the COBIT framework should be added as inherent IT security risks within the IT security risk register. • Define Key Risk Indicators (KRIs) including the associated thresholds. KRI data are normally sourced from people in the tactical management tier (e.g. CIO's direct reports). • Define the controls for each identified risk; assess each of the controls' adequacy and effectiveness. • Assess the risk once the controls have been taken into consideration, and record the residual risk as the risk that is tracked on a regular basis in the IT security risk register.		
TOOLS	• Workshops (Senior & tactical management) • Spreadsheets • Word documents	• COBIT • OCTAVE • RCSA (Risk & Control Self-Assessment) and KRIs		• Centralised document management application (e.g. Microsoft SharePoint)
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table 5.4 – ITSRB Approach Phase 2

PHASE 2	**DO:** IMPLEMENT THE ITSRB APPROACH		
OBJECTIVE	The objective of this phase is to put the ITSRB approach into effect within a specific organisation. Implementing the ITSRB approach will enable IT security professionals to prioritise implementation of the necessary IT security controls as per the organisation's risk profile.		
FREQUENCY	Quarterly		
TARGET AUDIENCE	• Tactical Management • Operational Management		
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**
	• IT security risk register • IT components (i.e. information, hardware, software, procedures, networks, people) • Previous IT security incident report	For each risk within the IT security risk register: • Identify and define each IT component(s) affected by each risk. • Decompose each identified IT component. • Categorise the identified sub-components (i.e. High\Med\Low based on business criticality). • Identify current threats for each IT sub-component. • Document the threats for each IT sub-component. • Select IT security controls for each IT sub-component commensurate with the threat. • Plan the implementation of the IT security control(s) as per the IT budget. • Prioritise implementation basing the decision on the risk impact to the business and IT operations.	• IT security risk register (updated) • IT security threat landscape

PHASE 2	**DO:** IMPLEMENT THE ITSRB APPROACH			
		• Implement IT security control(s) for each IT sub-component as the per the implementation plan. • Assess the IT security control(s) for each identified asset and update the IT security risk register on a regular basis. • Monitor the IT security control(s) for each identified asset.		
TOOLS	• Focused workshops/meetings with IT management (i.e. CIO's direct reports, their subordinates) and other relevant operational staff • Spreadsheets • Word documents	• ITIL and ISO 27001 • OCTAVE • RCSA, Management Actions, KRIs and Operational losses		• Centralised document management application (e.g. Microsoft SharePoint)
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table 5.5 – ITSRB Approach Phase 3

PHASE 3	**CHECK:** MONITOR THE ITSRB APPROACH		
OBJECTIVE	The objective of this phase is to monitor the adequacy and the performance of the ITSRB approach. Performing this phase will assist the organisation to reflect on how the ITSRB is doing, thereby highlighting the good and the bad IT security risk areas for the IT environment.		
FREQUENCY	Monthly		
TARGET AUDIENCE	• Tactical Management • Operational Management		
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**
	• IT security risk register	For each risk within the IT security risk register: • Assess the adequacy and effectiveness of the IT security control(s) taking into consideration the IT security incidents associated with each risk as well as the key risk indicators. • Record the performance of the KRIs. • Record any operational losses for each risk which materialised during that specific month. • Update the Management Actions. • Update the residual risk. • Develop an IT security risk report which provides both a summarised view and a detailed view of the IT security risk profile. Update the IT security report on a monthly basis. • Record any generic areas of improvement of the ITSRB	• IT security risk register (updated) • IT security monthly report

PHASE 3	**CHECK:** MONITOR THE ITSRB APPROACH			
		approach and also include them in the IT security monthly report.		
TOOLS	• Focused workshops/ meetings with IT management (i.e. CIO's direct reports, their subordinates) and other relevant operational staff • Spreadsheets • Word documents	• RCSA, Management Actions, KRIs and Operational losses		• Centralised document management application (e.g. Microsoft SharePoint)
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table 5.6 – ITSRB Approach Phase 4

PHASE 4	**ACT:** MAINTAIN AND IMPROVE THE ITSRB APPROACH		
OBJECTIVE	The objective of this phase is to assess the performance of the ITSRB approach by identifying areas of improvement and then implementing corrective actions.		
FREQUENCY	Bi-annually		
TARGET AUDIENCE	• Strategic Management • Tactical Management		
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**
	• IT security monthly report • IT security strategy • IT security risk appetite • IT security risk profile	• Assess the trend of the IT security risks for six months and update the IT security risk profile. • Review the IT security risk appetite and update it (i.e. take guidance from the CIO and direct reports). • Review if the goals within the IT security strategy are being met. • Create a progressive report providing a view of the progress on the activities involved with regard to delivering against the IT security strategy. Define a generic plan of the activities which still need to be performed and record them in the organisation's action plan for IT security. • Present the report to strategic and tactical management.	• IT security progress report (bi-annual) • Action plan for IT security

PHASE 4	**ACT:** MAINTAIN AND IMPROVE THE ITSRB APPROACH			
TOOLS	• Centralised document management application (i.e. spreadsheets, word documents)	• Spreadsheets • Word documents • Powerpoint presentations		• Meetings with strategic and tactical management
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

5.5. CONCLUSION

This chapter presented the ITSRB approach. The comparative analysis of the different IT security frameworks and standards that are commonly used within various South African financial institutions was presented. The objective of presenting the comparative analysis was to summarise the key characteristics of each framework and to highlight the common factors amongst the discussed frameworks and standards. Subsequently, the attributes that make up the ITSRB approach were discussed to highlight their importance in managing IT security risk. Lastly, the different phases of the ITSRB approach were presented.

The following chapter discusses the data analysis process of this study which presents the findings of the survey carried out as part of the research strategy.

6. DATA ANALYSIS

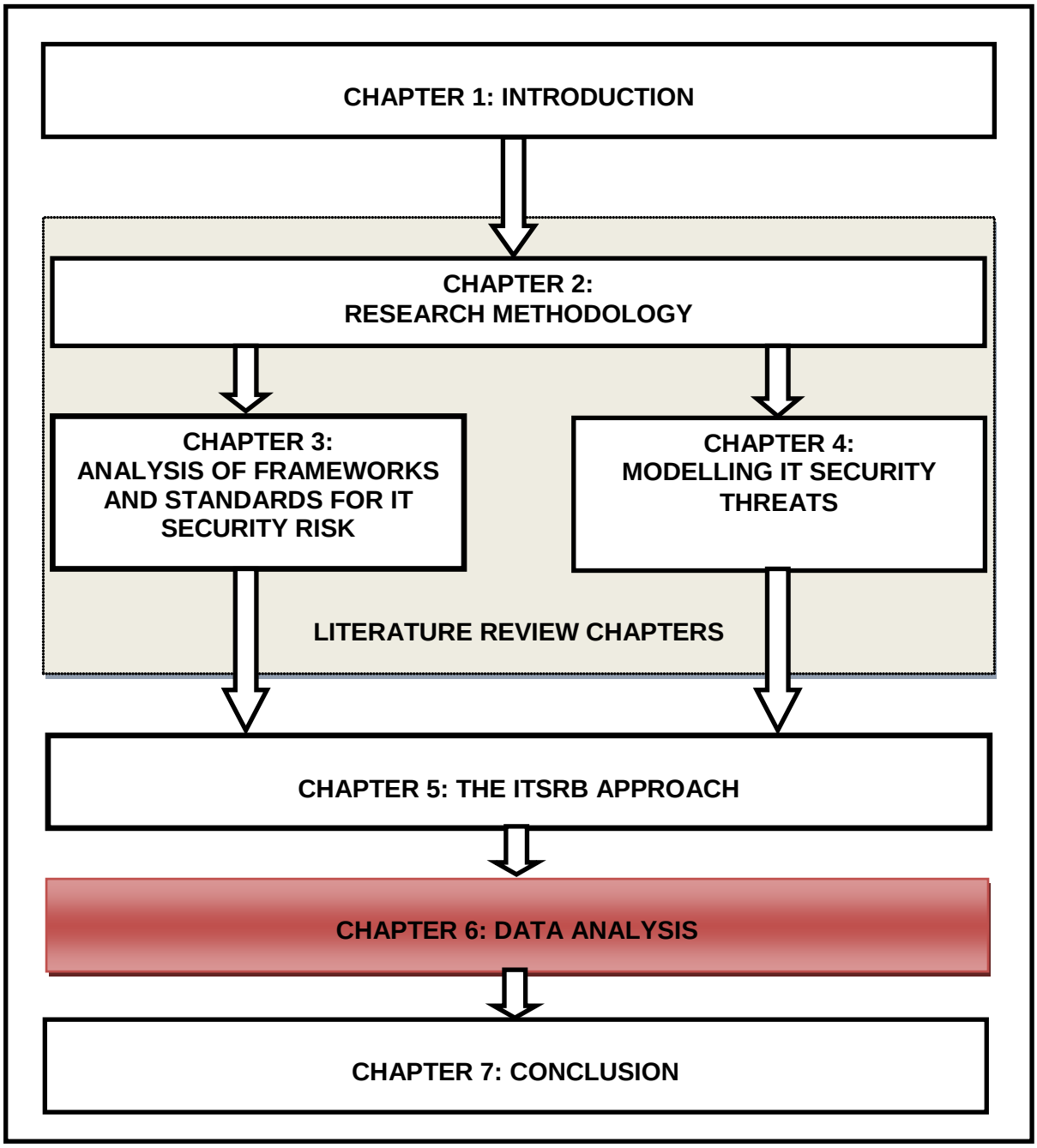

Figure 6.1 – Dissertation Layout: Chapter 6

6.1. INTRODUCTION

The foregoing chapter outlined the data collection process used in this study. The objective of this chapter is to present the findings of the survey as well as analyse the results of the findings in order to determine the respondents' level of agreement with the proposed ITSRB approach. As demonstrated in Chapter 6, the questionnaire was directly linked to the research objectives and research questions. Linking the questionnaire to the research objective and research questions ensured that relevant questions were posed to assist in making conclusions about the relevance of the ITSRB approach in the field of IT security.

Similarly, to ensure that the proposed ITSRB approach aligns with the research objectives and the questionnaire, phases of the ITSRB approach were mapped accordingly. Figure 6.2 depicts the research objectives, questionnaire and the ITSRB approach mapping. It becomes apparent in Figure 6.2 that the four phases of the ITSRB approach, namely, plan the ITSRB approach; implement the ITSRB approach; monitor the ITSRB approach; and maintain the ITSRB approach are aligned to the questionnaire as well as the research objectives of this study. Section 6.2 presents the findings as collected from SurveyMonkey including the analysis of those findings. The chapter is concluded in section 6.3.

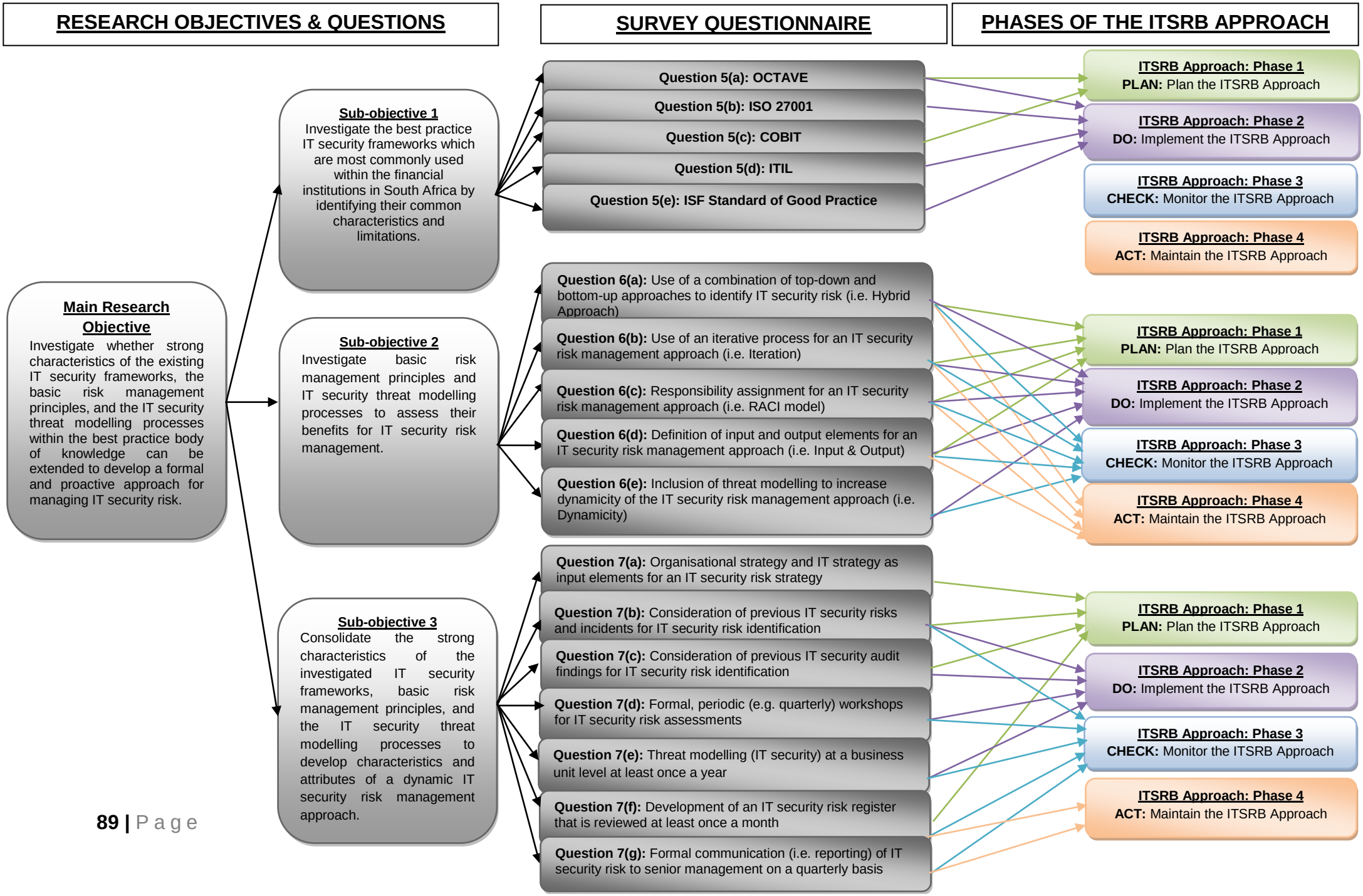

Figure 6.2 – Mapping of Research Objectives to the ITSRB Approach

6.2. FINDINGS

To achieve a 90% confidence level and a 10% margin of error, the final sample size had to be at least 60 responses. As indicated in Chapter 6, the questionnaire was sent to 150 IT security professionals. The intention of sending the questionnaire to 150 respondents was to ensure that the final sample of at least 60 respondents to attain an adequate confidence level and low margin of error is achieved. An overview of the response summary sourced from SurveyMonkey is presented in Figure 6.3.

Figure 6.3 – Questionnaire Response Summary

Penwarden (2014) indicated that an average response rate for a survey such as this one is 24.8%. A total number of 65 responses were received through SurveyMonkey, which provided a response rate of 43%. Out of the 65 respondents, one respondent did not complete all of the questions required to be answered, and the other respondent either exited the survey half way or did not attempt to answer some of the questions. This implies that the total number of responses considered for analysing the findings is 63. As per the selected confidence level of 90% and a margin of error of 10%, it is safe to conclude that the responses received for this survey were sufficient to satisfy the research objective and research questions.

6.2.1. Findings for section 1 of the questionnaire: General information

Section 1 assessed the demographics of the sample group in order to determine if they actually met the predefined characteristics of the target population. As indicated in Chapter 2, the target population included IT security professionals within South African financial institutions.

6.2.1.1. Question 1: Section 1 of the questionnaire

Question 1 of the questionnaire determined the size of the organisation that the respondents worked for. This information indicates the percentage of respondents who come from large and complex environments. An assumption made is that, if the ITSRB approach is able to add value to large organisations which are more complex, it will also add value to medium and small organisations which are less complex. Ideally, more respondents who work for large organisations would be able to add more value to the survey. Figure 6.4 depicts the response summary for question 1 of the questionnaire.

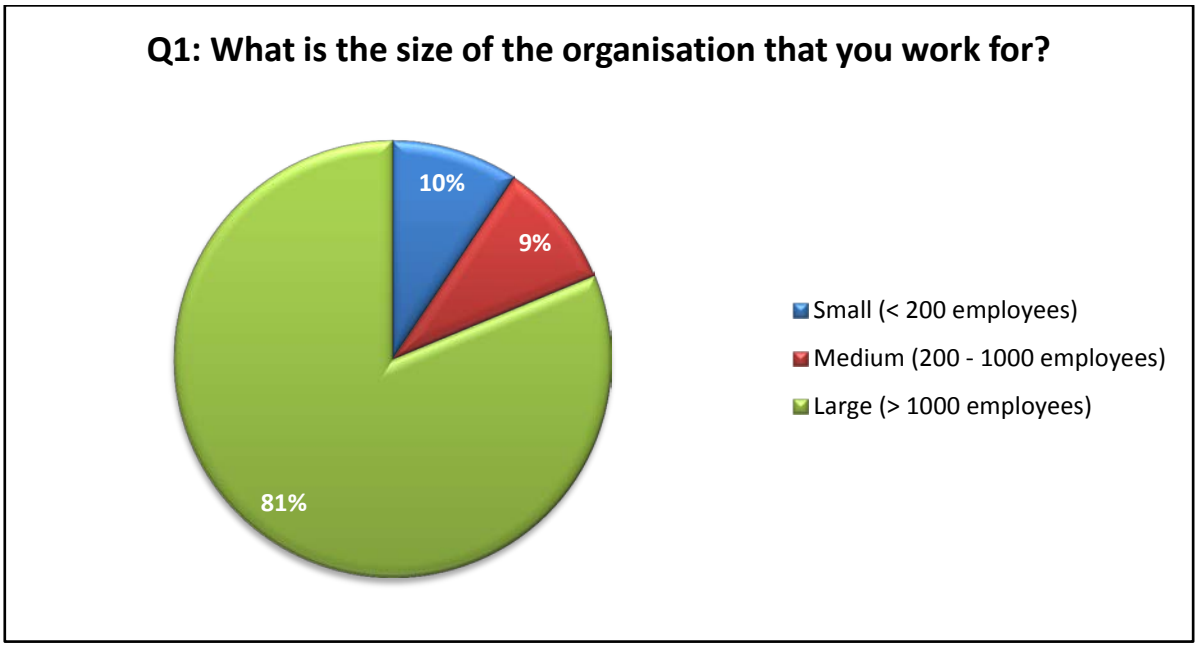

Figure 6.4 – Question 1 Response Summary

Figure 6.4 indicates that 81% of the respondents come from large organisations, with 9% from medium organisations and the remaining 10% from small organisations. The results show that the majority of the respondents work in large organisations

that have complex environments. The view of the respondents about the attributes and characteristics of the ITSRB approach carries more weight to the conclusions made, as they are viewing the ITSRB approach from a complex environment perspective.

6.2.1.2. Question 2: Section 1 of the questionnaire

Question 2 of the questionnaire determined if the respondents were responsible for managing IT security risk, directly or indirectly. Respondents whose responsibility include management of IT security risk would add value to the survey because they would understand IT security concepts used for this study. Figure 6.5 presents the response summary for question 2 of the questionnaire.

Figure 6.5 – Question 2 Response Summary

Figure 6.5 reveals that 98% of the respondents indeed work in an area which directly or indirectly manages IT security risk. Two percent of the respondents do not work in an environment where they manage IT security risk directly; however, the comment provided states that the environment that the respondents work in is an IT Audit function which also incorporates IT security audits. It is therefore safe to conclude that all the respondents are involved directly or indirectly with management of IT security risk, implying that these individuals will comprehend the IT security concepts used in the questionnaire.

6.2.1.3. Question 3: Section 1 of the questionnaire

Under normal circumstances, IT security functions within large organisations have different focus areas such as operations, governance, risk management, and monitoring. The objective of this question was to get an indication of the demographics of the respondents in order to get a high-level view of their IT security focus areas. Figure 6.6 highlights the response summary for question 3 of the questionnaire.

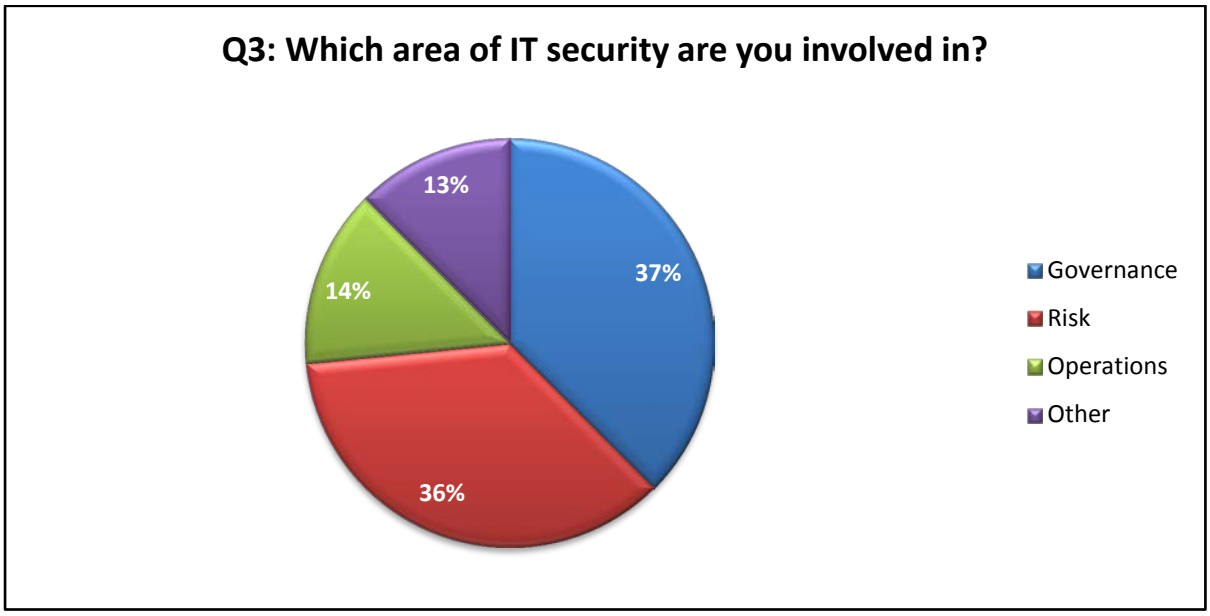

Figure 6.6 – Question 3 Response Summary

Figure 6.6 illustrates that 37% of the respondents work in IT security governance, 36% works in IT security risk, 14% in IT security operations, and 14% in other areas (i.e. indicated as security architecture, security consulting and security sales). This demonstrates that there is an adequate mix of respondents who participated in the survey. Having a mix of respondents adds value to the survey, as the respondents assess the ITSRB approach from different perspectives.

6.2.1.4. Question 4: Section 1 of the questionnaire

A general assumption is that people with more work experience have more knowledge about a specific subject. Question 4 of the questionnaire assessed the level of IT security experience of the respondents. Figure 6.7 depicts the response summary for question 4 of the questionnaire.

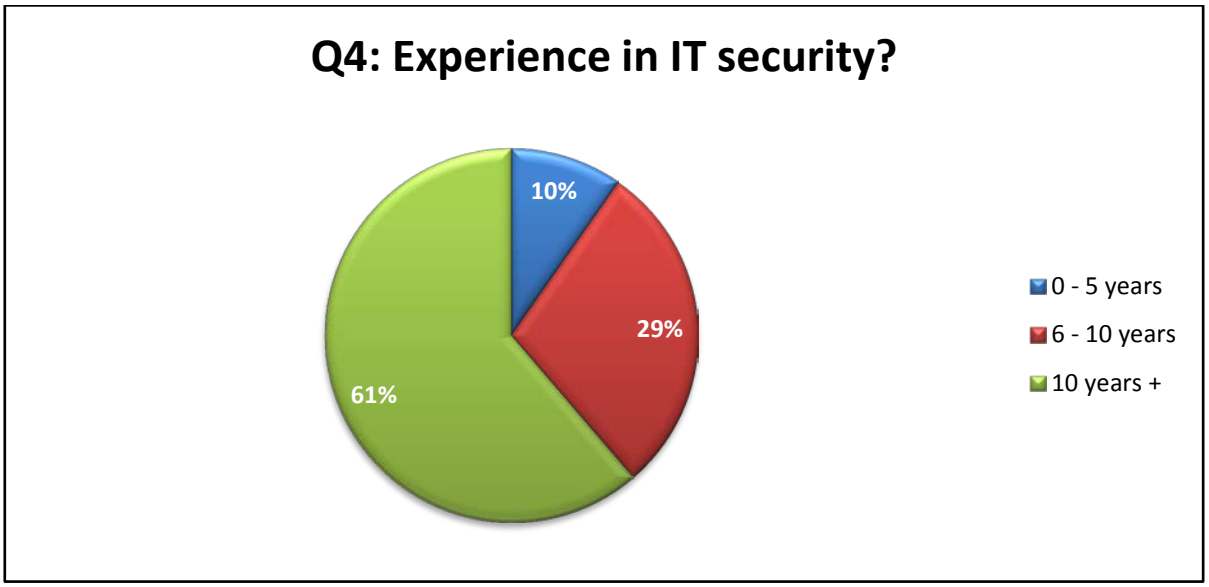

Figure 6.7 – Question 4 Response Summary

Figure 6.7 shows that the majority of the respondents have over five years' experience in the field of IT security. It is safe to assume that the sample group consisted of enough respondents that have extensive knowledge in the field of IT security to assess the characteristics of the ITSRB approach adequately.

6.2.1.5. Summary for section 1 responses

Analysis of section 1 indicates that the respondents are in the correct target population. They work for large organisations and in one of the disciplines of IT security. Based on the findings presented in this section, it is safe to conclude that the respondents from the sample group are adequate in assessing the ITSRB approach and its applicability within the organisations they work for.

6.2.2. Findings for section 2 of the questionnaire: Best practice IT security frameworks and standards

Section 2 of the questionnaire evaluated the respondents' views on the different IT security frameworks and standards that are commonly used within South African financial institutions. The goal of this section was to determine the respondents' views on the selected frameworks and standards' ability to manage IT security risk. Furthermore, the questions in this section link directly to research sub-objective 1 and research question 1 *(i.e. Do the selected best practice IT security frameworks and standards most commonly used within the financial institutions in South Africa assist in managing IT security risk?)* presented in Figure 6.2. The following request was presented in the questionnaire for this section: **"*indicate your opinion on the IT security risk management frameworks and standards used in defining the proposed approach*".** Figure 6.8 presents the response summary for section 2 of the questionnaire.

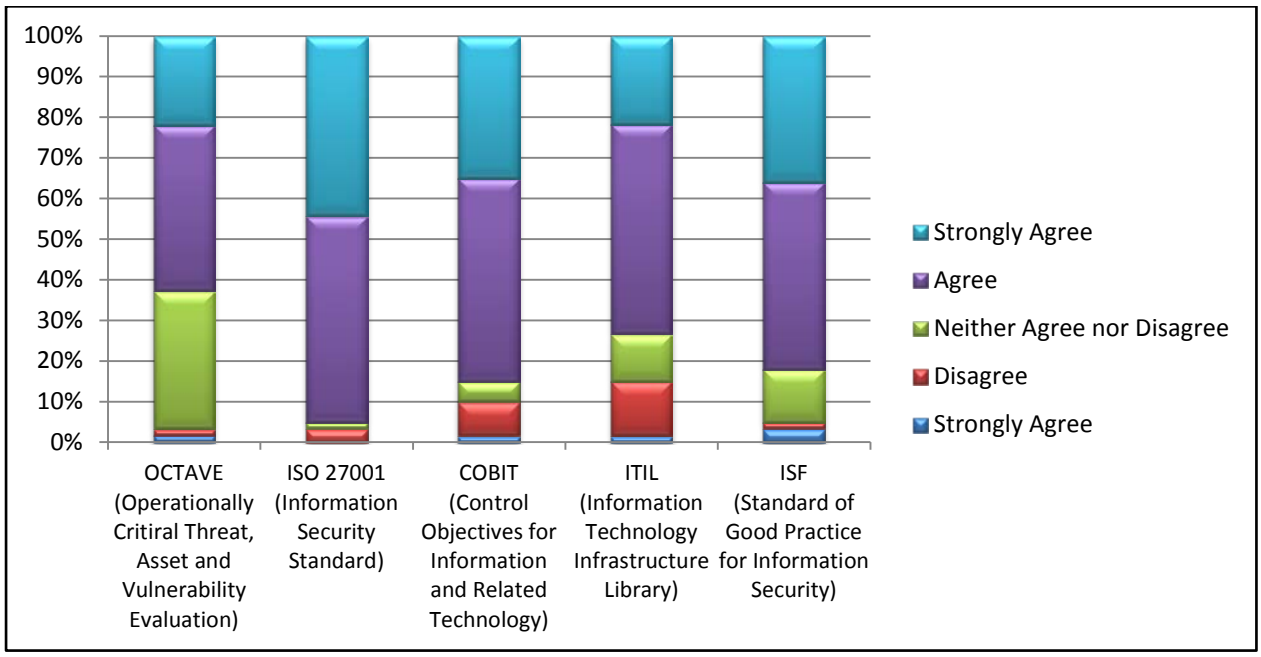

Figure 6.8 – Section 2 Response Summary

Section 2 comprises question 5(a), question 5(b), question 5(c), question 5(d) and question 5(e), also indicated in Figure 2.4. Figure 6.8 indicates that the majority of the respondents agreed with the statements. The individual questions of this section are discussed in Section 6.2.2.1 to Section 6.2.2.5.

6.2.2.1. Question 5(a): Section 2 of the questionnaire

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a process-driven framework that enables organisations to understand, assess and address their IT security risks from an organisation's perspective (Panda, 2009). OCTAVE was selected as one of the frameworks investigated for this study because of its ability to engage the entire organisation for IT security risk assessments. The level of agreement from the respondents with the fact that OCTAVE can be used by organisations to manage their IT security was determined in this question. Figure 6.9 depicts the response summary for question 5(a) of the questionnaire.

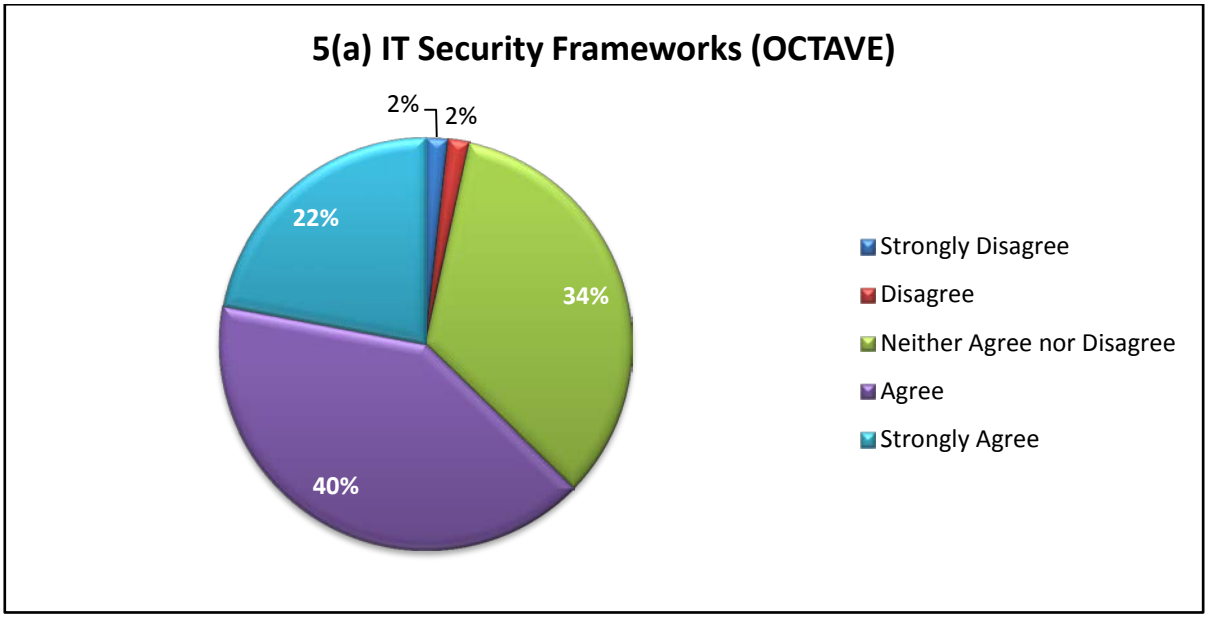

Figure 6.9 – Question 5(a): OCTAVE

Figure 6.9 reveals that 62% (i.e. 22% strongly agree and 40% agree) of the respondents agree that OCTAVE is a good framework to manage IT security risk. As much as OCTAVE is a fairly known IT security risk management framework, there are many people from the sample group who do not know about it. Thirty-four per cent of the respondents neither agree nor disagree, which potentially implies that they have never used OCTAVE before. Four per cent of the respondents disagree (i.e. 2% disagree and 2% strongly disagree) with the fact that OCTAVE can assist in managing IT security risk.

Based on the results of this question, it is assumed that OCTAVE is not commonly used by the respondents. The fact that only 62% of the respondents agree with the fact that OCTAVE can assist in managing IT security risk alludes to this conclusion. However, this does not mean that OCTAVE does not employ good principles which are good for managing IT security risk within organisations.

6.2.2.2. Question 5(b): Section 2 of the questionnaire

Question 5(b) assessed the respondents' views on ISO 27001. ISO 27001 provides guidance to organisations on how to implement security controls in order to accomplish security objectives of safeguarding confidentiality, integrity and availability of information and systems (ISO 27001, 2007). ISO 27001/2 does not explicitly apply risk management principles; however, the literature review revealed that application of the recommended controls can assist in mitigating IT security risks. ISO 27001/2 was selected because it provides a detailed list of security controls that align with business requirements and the fact that it is one of the well-known frameworks used across the globe for IT security benchmarking purposes. Figure 6.10 depicts the response summary for question 5(b) of the questionnaire.

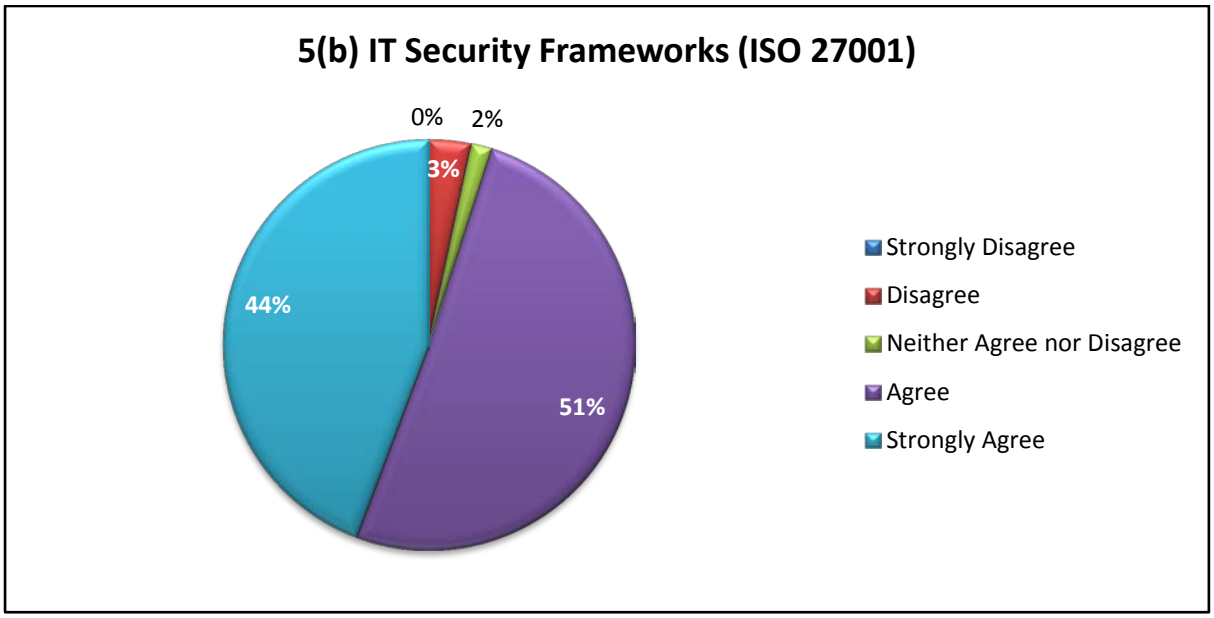

Figure 6.10 – Question 5(b): ISO 27001

Figure 6.10 illustrates that the majority of the respondents agree with the fact that ISO 27001 can be used to manage IT security risk. The majority of the respondents

agreed with this statement (i.e. 51% agree and 44% strongly agree) implying that the majority of the respondents have potentially used it before.

Even though the majority of the respondents agree that ISO 27001 can manage IT security risk, there is still a minority (i.e. 5%) that disagrees. Based on these results, it is safe to conclude that the security controls recommended by ISO 27001 can assist in managing IT security risk if applied correctly.

6.2.2.3. Question 5(c): Section 2 of the questionnaire

As discussed in Chapter 3, COBIT 5 provides guidance on what processes and controls should exist within an IT division of an organisation, with only a subset of COBIT 5 focusing on IT security. Implementing an IT governance framework correctly within an organisation provides many benefits, one of which is effective management of IT security risk (IT Governance Institute [ITGI], 2012). COBIT 5 was investigated because it provides a view of the processes and controls that are essential for an IT environment, thereby making a link to the business requirements and encouraging responsibility assignment. Figure 6.11 depicts the response summary for question 5(c) of the questionnaire.

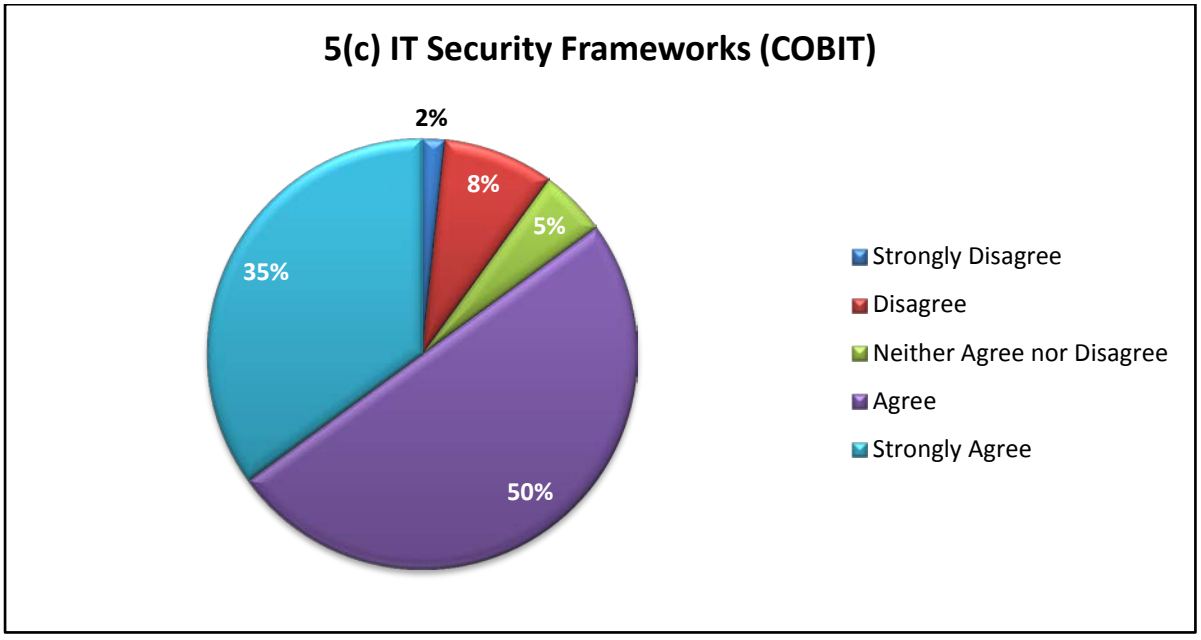

Figure 6.11 – Question 5(c): COBIT

Figure 76.11 indicates that even though there is a significant number of respondents who agree with the use of COBIT for IT security risk management, there is still a substantial number of respondents who disagree with the use of COBIT for IT security risk management. The questionnaire did not provide a field that allowed the respondents who are not in agreement with the opportunity to provide the reasons thereof.

COBIT is predominantly an IT governance framework; hence, it is good when an organisation wants to define the controls and processes that should make up their IT environment. Based on the results depicted in Figure 6.11, it is safe to conclude that COBIT has some good characteristics which may be applied in managing IT security risk.

6.2.2.4. Question 5(d): Section 2 of the questionnaire

The literature review in Chapter 3 discussed ITIL in detail. The literature indicated that ITIL is also an IT governance framework that is used mostly within the IT operations area. ITIL's primary focus is the IT service life cycle, which implies that it does not solely focus on IT security. For this reason, ITIL might not be strong in most aspects of managing IT security risk. Nevertheless, it is important to note that the governance principles recommended by ITIL indirectly assist in mitigating IT security risk; as such, it was selected for this study. Figure 6.12 illustrates the response summary for question 5(d) of the questionnaire.

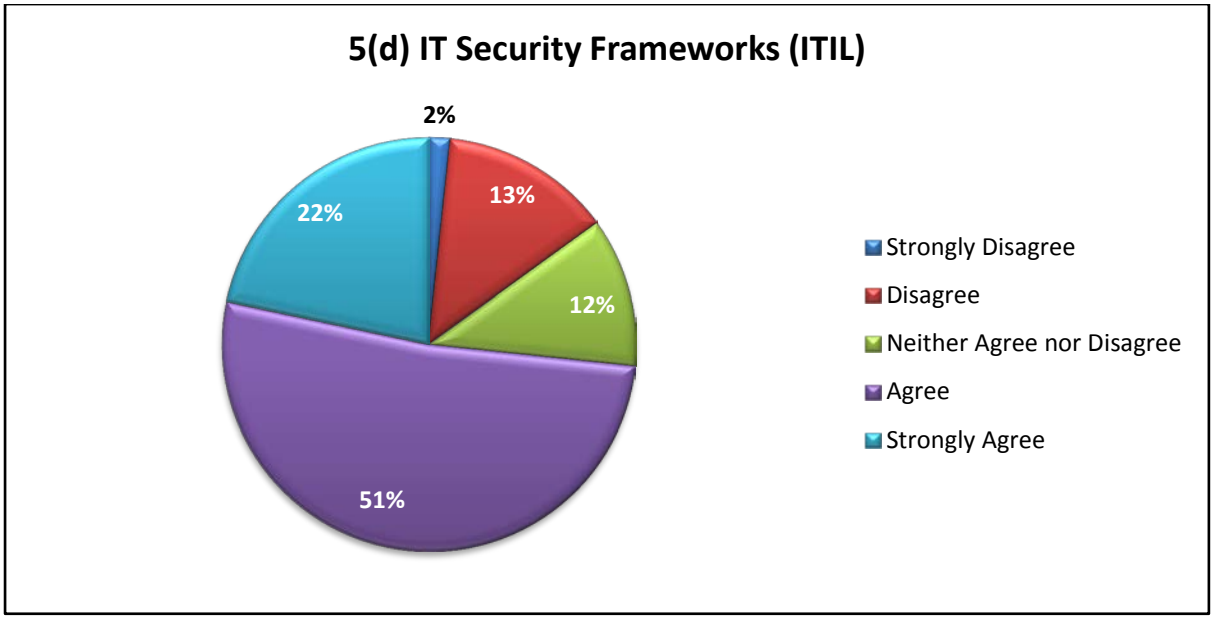

Figure 6.12 – Question 5(d): ITIL

Once again, as demonstrated in Figure 6.12, the majority of the respondents agree that ITIL can be used to manage IT security risk (i.e. 22% strongly agree and another 51% agree). Twelve per cent of the respondents neither agree nor disagree. In contrast, 15% of the respondents disagree with the fact that ITIL can assist in managing IT security risk.

Because the majority of IT activities within an organisation take place in the IT operations area, most IT security incidents are also found there (IT Service Management Forum [ITSMF], 2007). To ensure that proper governance controls are in place, a framework such as ITIL can provide significant value in guiding the IT operational activities better (ITSMF, 2007). For this reason, IT security risk gets to be better managed when a good IT governance framework is effective. An assumption is made that even though ITIL's primary focus is not IT security, it can still assist in managing IT security risk to a certain degree.

6.2.2.5. Question 5(e): Section 2 of the questionnaire

As its title suggests, the ISF Standard of Good Practice (SoGP) provides a detailed best practice set of controls which covers the IT environment holistically, minimising the need to purchase an additional repository of potential controls (Chaplin & Creasy, 2011). The ISF SoGP is one of the well-known standards across the globe

within the field of IT security, and it is also commonly used for benchmarking purposes, as discussed in Chapter 3. The ISF SoGP provides IT security controls and does not explicitly present a specific risk management process. It was selected for this study because of its rigour and ease of integration with other frameworks. Figure 6.13 shows the response summary for question 5(e) of the questionnaire.

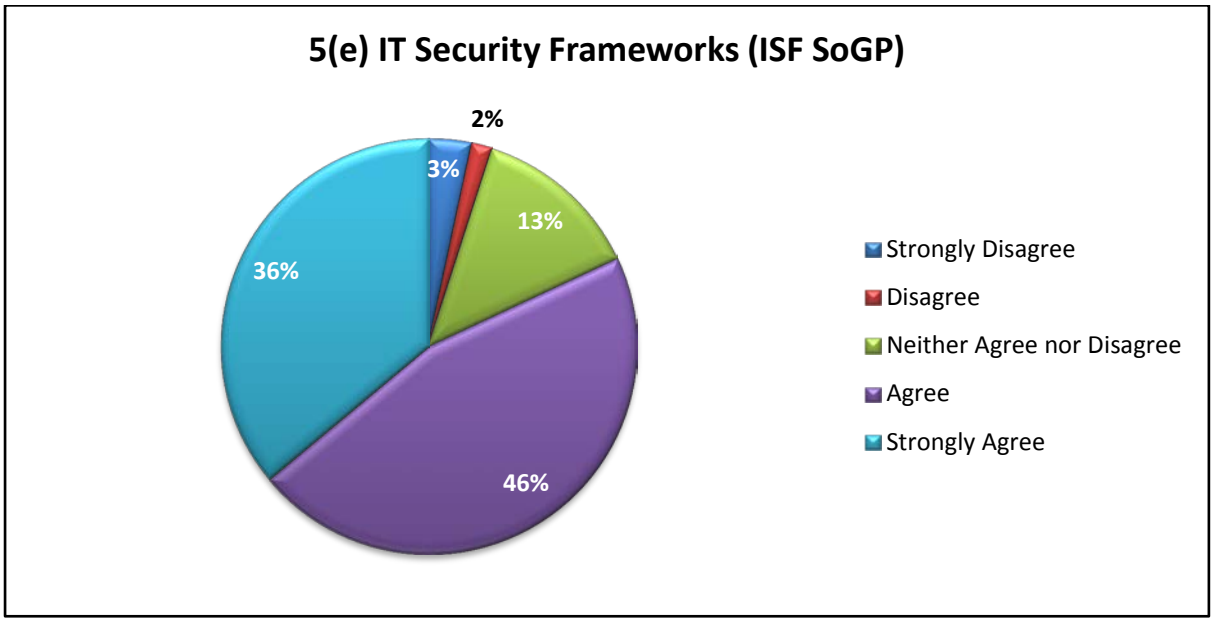

Figure 6.13 – Question 5(e): ISF SoGP

Figure 6.13 reveals that 82% of the respondents agree with the fact that ISF SoGP can be used to manage IT security risk (i.e. with 46% agreeing and 36% strongly agreeing). ISF SoGP is solely focused on IT security, hence its high popularity within the IT security community. Figure 6.13 also demonstrates that 5% of the respondents disagree that ISF SoGP is good in managing IT security risk. On the other hand, 13% of the respondents neither agree nor disagree, which may imply that they have never used it before or that they do not know it. Once again, it is concluded that ISF SoGP can be used to manage IT security risk.

6.2.2.6. Summary for section 2 responses

The five frameworks and standards assessed in this section are some of the most common frameworks and standards used within the field of IT security. The results have indicated that even though a minority of the respondents disagree with some of the frameworks and standards, there is still a majority of the respondents who agree

that the discussed frameworks and standards can be used to manage IT security risk. This proves that there are some good elements about the frameworks and standards discussed and there are some elements which other users do not prefer, hence the purpose of this study.

Because section 2 of the questionnaire aimed to determine if frameworks and standards investigated possess good characteristics for managing IT security risk, it is therefore safe to conclude that this goal was achieved. Research sub-objective 1 has been achieved because the majority of the respondents showed a fairly consistent level of agreement for the statements presented by the questionnaire.

6.2.3. Findings for section 3 of the questionnaire: Approach to IT security

It is indicated in Chapter 3 that there are various approaches which can be applied in managing IT security risk. The objective of this section was to assess the respondents' views with respect to the approach they use in managing IT security risk in comparison to the attributes used to define the ITSRB approach. Moreover, the questions in this section linked directly to research sub-objective 2 and research question 2 *(i.e. Can best practice risk management principles and IT security threat modelling processes be adopted for IT security risk management?)* presented in Figure 2.4. The following request was presented in the questionnaire: **"*indicate your opinion on the primary attributes of the proposed approach*".** Figure 6.14 presents the response summary for this section.

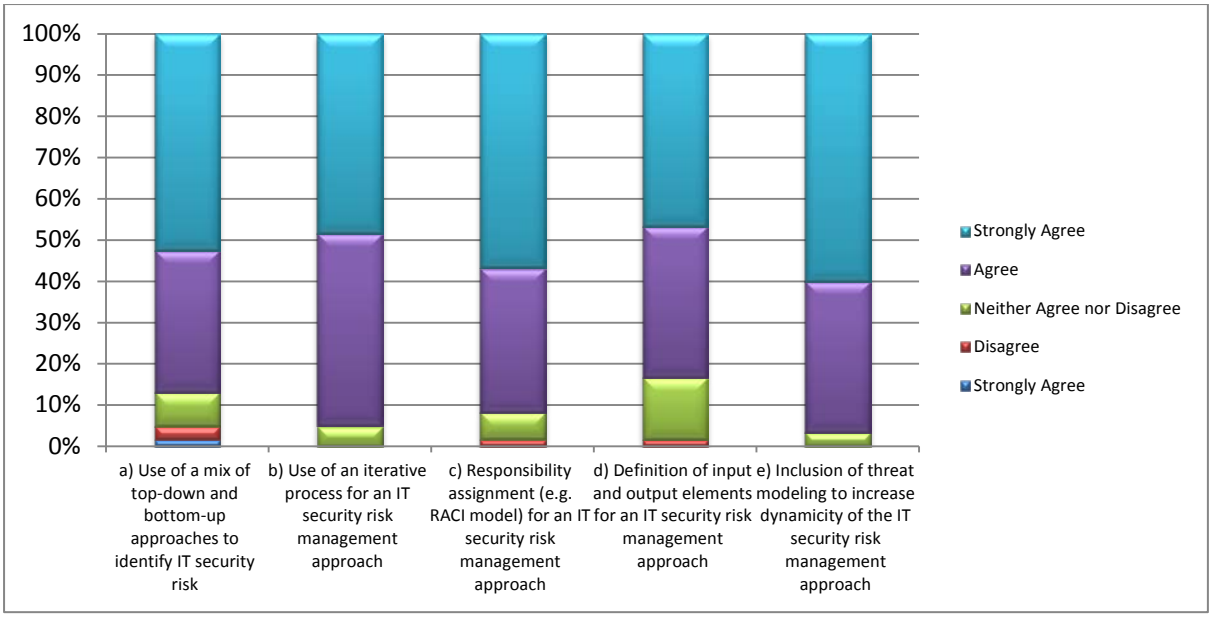

Figure 6.14 – Section 3 Response Summary

Figure 6.14 illustrates that section 3 of the questionnaire comprised five sub-questions, namely, question 6(a), question 6(b), question 6(c), question 6(d) and question 6(e), also indicated in Figure 6.2. The individual questions for this section are discussed in Section 6.2.3.1 to 6.2.3.5.

6.2.3.1. Question 6(a): Section 3 of the questionnaire

To ensure the correct coverage of IT security risk, assessment of risk should be conducted at a strategic, tactical and operational levels of management (National Institute of Standards and Technology [NIST], 2010). Question 6(a) assessed the level of agreement from the respondents regarding the use of a combination of a top-down approach (i.e. from strategic level down to operational level) as well as the bottom-up approach (i.e. from operational level up to strategic level) in managing IT security risk. This attribute is also termed the hybrid approach in Chapter 5 and was derived from the OCTAVE framework, as it allows for the entire organisation to be involved in management of IT security risk. Figure 6.15 depicts the response summary for question 6(a) of the questionnaire.

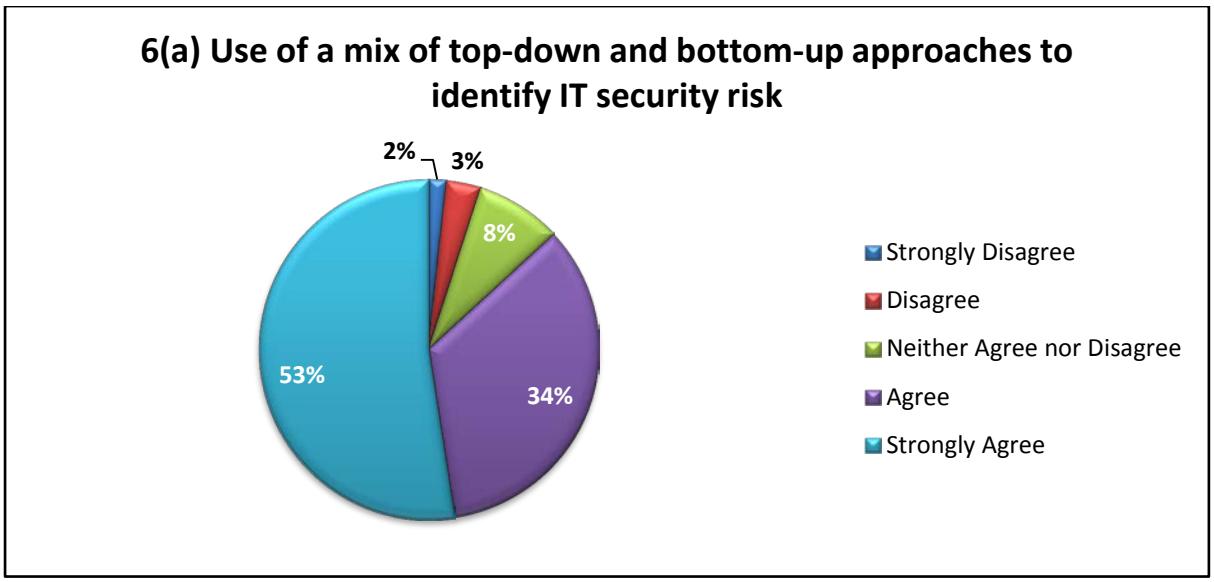

Figure 6.15 – Question 6(a): Top-down and Bottom-up Approach

Figure 6.15 highlights that the majority of the respondents agreed with the statement (i.e. 34% agree and 53% strongly agree with this statement). Only 8% of the respondents were neutral (i.e. neither agree nor disagree). The detailed analysis conducted in Chapter 3 pointed out that failure to manage risk from the top as well as risk from the operations of the IT environment could result in a one-sided view of the IT security risk profile. In the cases where risk is not identified and managed properly, there might be dire consequences. It is therefore safe to conclude that this attribute is good for effective IT security risk management.

6.2.3.2. Question 6(b): Section 3 of the questionnaire

ISO 31000 and all the selected IT security frameworks and standards emphasise the importance of iteration to ensure continuous improvement. Question 6(b) assessed the respondents' level of agreement respecting employing an iterative process to manage IT security risk. This attribute was also discussed in detail in Chapter 5. Figure 6.16 depicts the response summary for question 6(b) of the questionnaire.

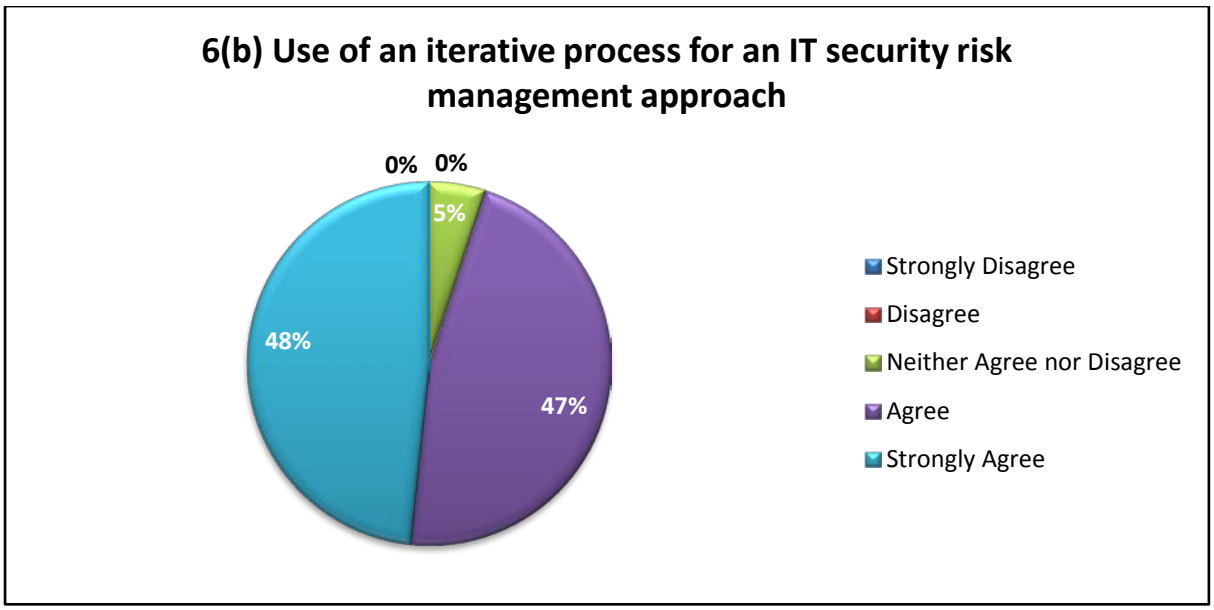

Figure 6.16 – Question 6(b): Iterative Process

The results as revealed in Figure 6.16 show that 95% of the respondents agree (i.e. 47% agree and 48% strongly agree) that an IT security risk management process should be iterative. Five per cent of the respondents did not agree nor disagree with this principle. Because the questionnaire was not designed in a way that provided the respondents with the opportunity to present their views on not agreeing with some of the statements, it was not possible to know the reasons from those respondents.

The reviewed literatureindicated the importance of iteration for IT security risk management. It is therefore safe to come to the conclusion that the principle of iteration is required for IT security risk management. Lack of an iterative process might result in unanticipated risk materialising, resulting in unforeseen consequences.

6.2.3.3. Question 6(c): Section 3 of the questionnaire

Banacorsi (2011) has demonstrated the importance of responsibility assignment for any task. Failure to explicitly assign a specific task to an individual may lead to ambiguity, thus resulting in a task not being executed or the task not receiving the correct level of attention (Smith & Erwin, 2005). Responsibility assignment is also deemed as one of the important principles of the COBIT framework, as discussed in Chapter 3. This matter was presented to the respondents in order to assess their

level of agreement with reference to the importance of responsibility assignment as part of an IT security risk management process. Figure 6.17 illustrates the response summary for question 6(c) of the questionnaire.

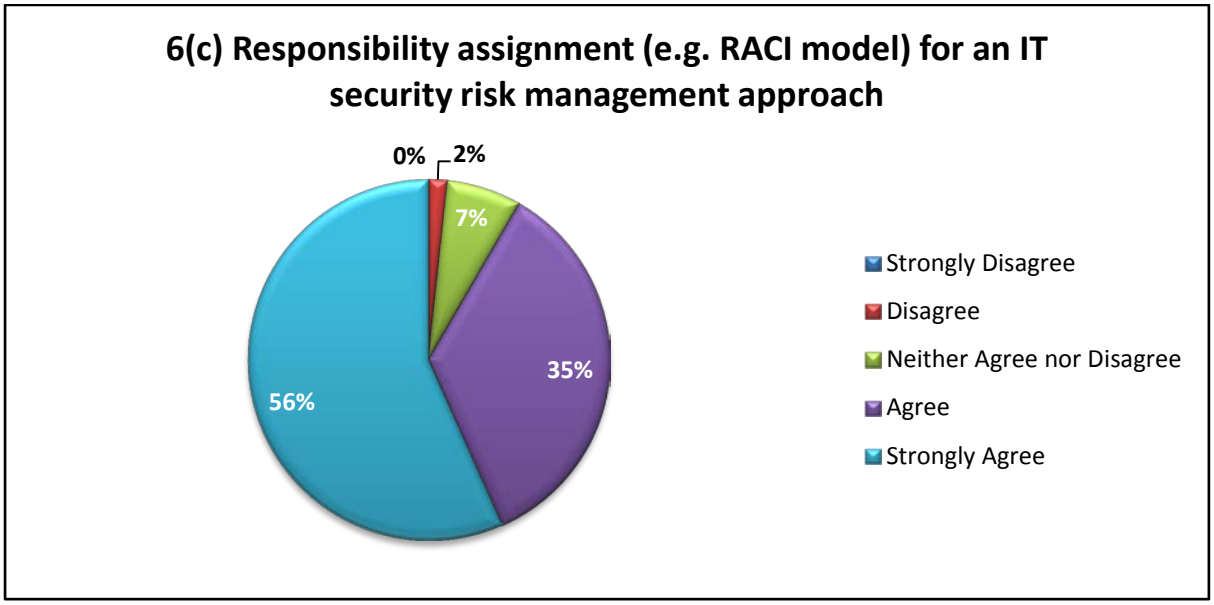

Figure 6.17 – Question 6(c): Responsibility Assignment

Figure 6.17 shows that the majority of the respondents agreed with this statement (i.e. 35% agree and 56% strongly agree). Seven per cent of the respondents neither agree nor disagree, whereas 2% of them disagree with the statement. Based on the high level of agreement from the respondents as well as the analysis conducted in Chapter 3, it is safe to conclude that responsibility assignment is a good attribute for IT security risk management.

6.2.3.4. Question 6(d): Section 3 of the questionnaire

It is imperative for any process to have input and output elements defined to manage expectation regarding what artefacts are required to execute and complete the respective processes (ITSMF, 2007). The objective of this question was to assess the respondents' level of agreement in comparison to the proposed approach about the importance of defining input and output elements as part of an IT security risk management process. This attribute was derived from the ITIL framework discussed in detail in Chapter 3. Figure 8.18 depicts the response summary for question 6(d) of the questionnaire.

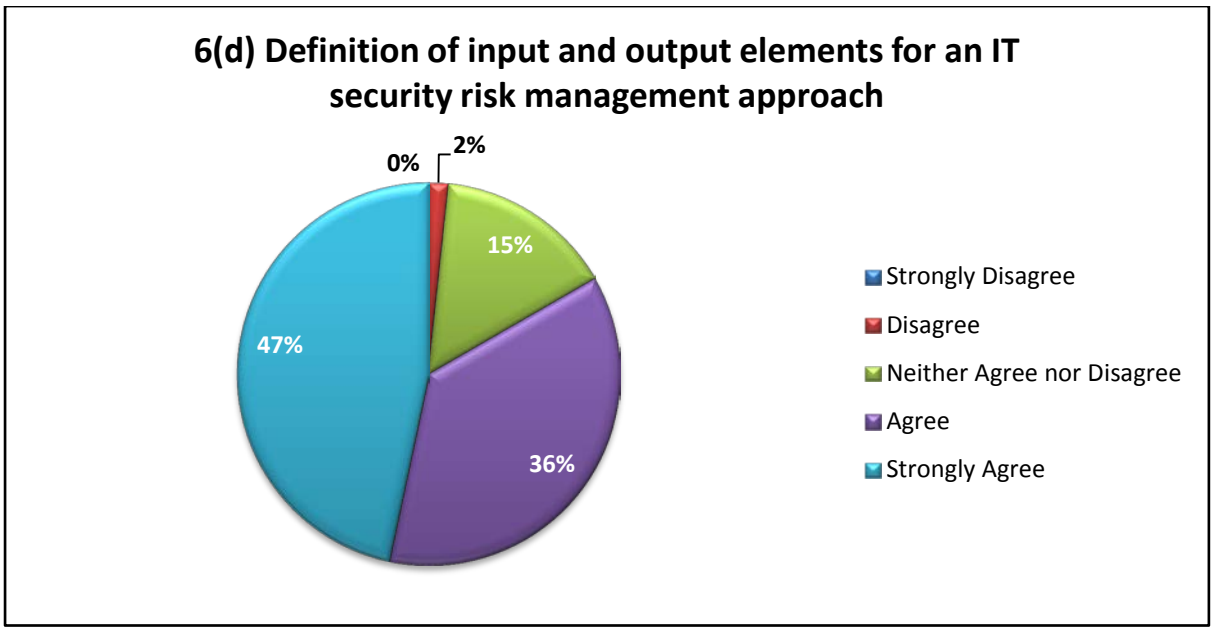

Figure 6.18 – Question 6(d): Input and Output Elements

Figure 6.18 presents the results from the respondents. It came to light that 36% of the respondents agree and 47% of the respondents strongly agree with this statement. However, 15% of the respondents neither agree nor disagree, while 2% of them disagree.

A number of tasks within organisations are not completed or are found to be poorly designed because the users do not know what they are meant to produce (Calder, 2013). The reviewed literature and the fact that over 80% of the respondents agree with this attribute implies that this principle is important. It is concluded that the task of defining input and output elements have a level of impact on the efficiency of an IT security risk management process.

6.2.3.5. Question 6(e): Section 3 of the questionnaire

IT is dynamic in nature; because of that, the threats associated with IT also change quite often (Winter & Schelp, 2008). The objective of this question was to assess the respondents' level of agreement regarding the inclusion of threat modelling during an IT security risk management process. The idea behind threat modelling is to ensure that the right risk that is facing an organisation is managed in a way that will provide the highest benefits possible (i.e. risk versus value). Figure 6.19 highlights the response summary for question 6(e) of the questionnaire.

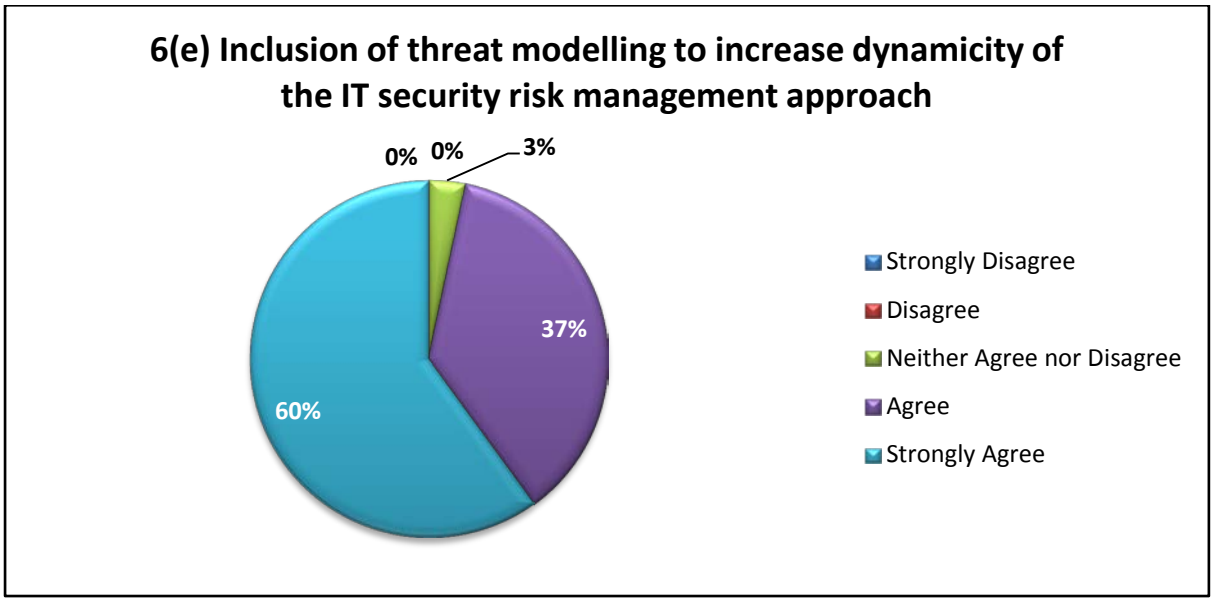

Figure 6.19 – Question 6(e): Threat Modelling

The majority of the respondents of this survey agree with the statement as indicated in Figure 7.19 (i.e. 60% strongly agree and 37% agree). As demonstrated in Chapter 4, the benefits of conducting threat modelling are enormous. Threat modelling provides its users with the ability to be more proactive and dynamic when managing IT security risk. It is therefore safe to conclude that it is important to cater for the nature of change associated with IT during an IT security risk management process.

6.2.3.6. Summary of section 3 responses

The five primary attributes of how to best approach IT security risk management were presented to the respondents. The responses indicate a positive trend by the majority of the respondents (i.e. strongly agree and agree). As previously highlighted, these attributes were sourced from the different best practice frameworks and consolidated to make up the primary attributes of the proposed ITSRB approach. Based on the foregoing, it is safe to deduce that the approach that is employed by the ITSRB approach to manage IT security risk possesses sound attributes which may assist organisations in managing this risk more effectively.

6.2.4. Findings for section 4: Key principles of the proposed IT security risk management approach

As discussed in Chapter 5, the ITSRB approach was defined in a way that ensured that essential principles derived from the best practice frameworks and standards are incorporated as the basic principles. The objective of this section is to determine the respondents' views about the derived principles of the ITSRB approach. Furthermore, the questions in this section linked directly to research sub-objective 3 and research question 3 *(i.e. Do the characteristics and attributes deduced from the investigated IT security frameworks and standards, risk management principles, and IT security threat modelling process provide a good base for a proactive and dynamic IT security risk management approach?)* presented in Figure 2.4. The request presented in the questionnaire was: **"*indicate your opinion on the key principles of the proposed approach*".** Figure 6.20 presents the response summary for this section.

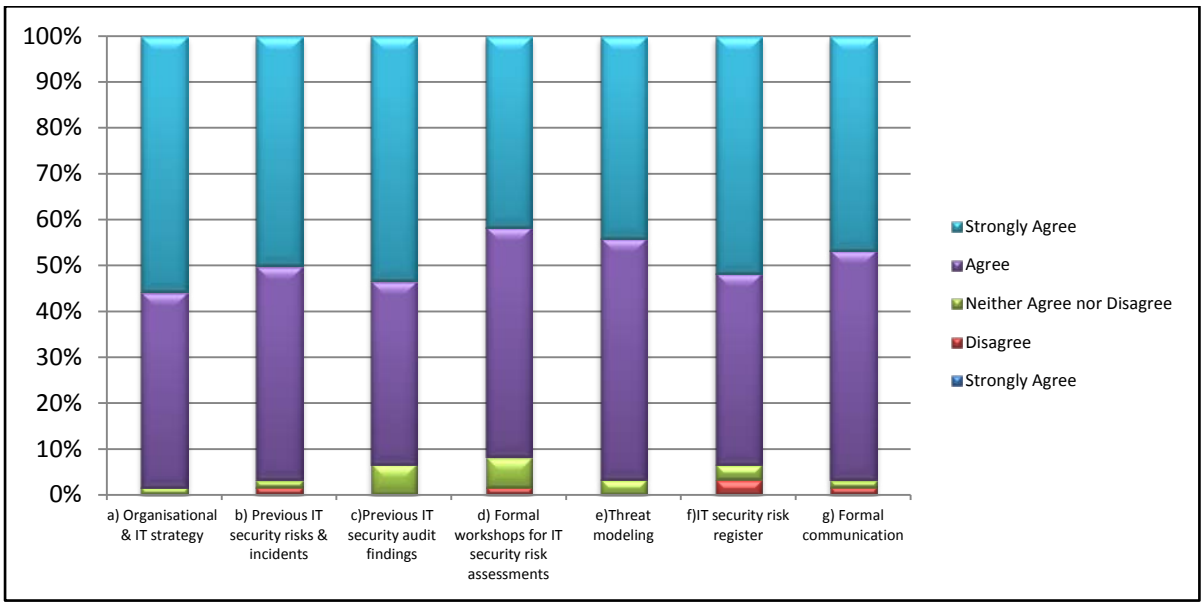

Figure 6.20 – Section 3 Response Summary

In Figure 6.20, it is indicated that section 4 of the questionnaire consisted of seven sub-questions, namely, question 7(a), question 7(b), question 7(c), question 7(d), question 7(e), question 7(f) and question 7(g), also presented in Figure 2.4. The individual questions for this section are discussed in Section 6.2.4.1 to 6.2.4.7.

6.2.4.1. Question 7(a): Section 4 of the questionnaire

The direction that any organisation follows is directed by the organisational strategy (Hill & Turbitt, 2006). Because IT is considered a custodian of business information, the strategy for IT should be fully aligned with the organisational strategy (Hill & Turbitt, 2006). Question 7(a) assessed the respondents' views about using the organisational strategy as well as the IT strategy in defining the IT security strategy. Figure 6.21 depicts the response summary for question 7(a) of the questionnaire.

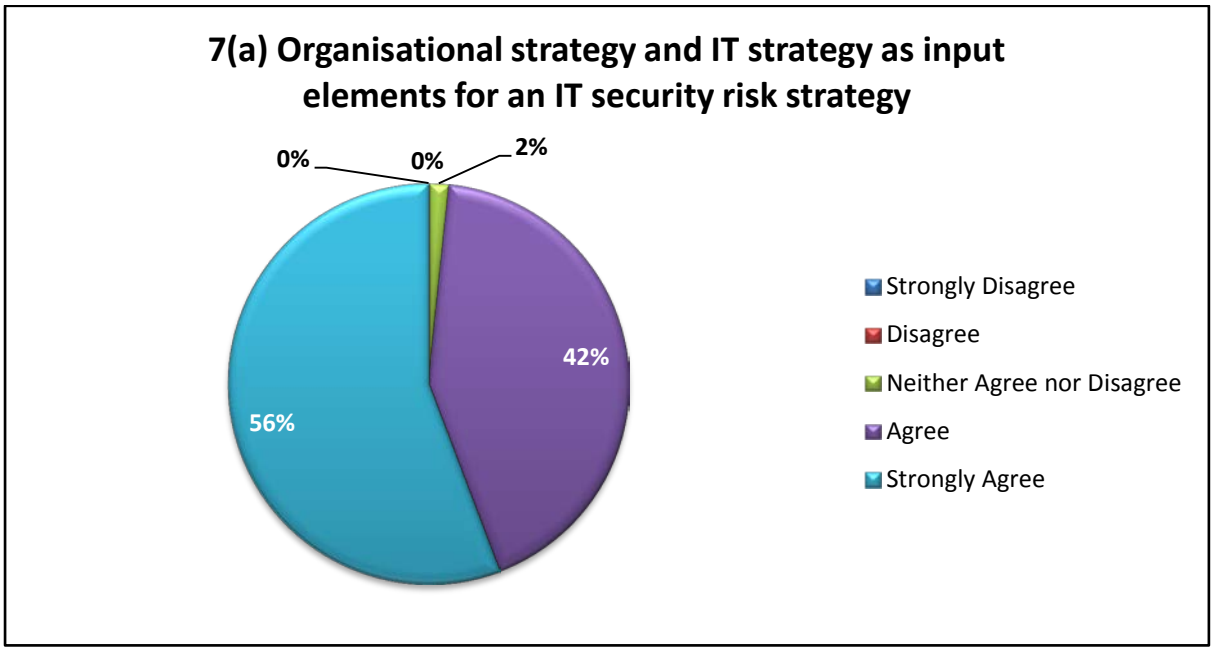

Figure 6.21 – Question 7(a): IT Security Strategy

The results shown in Figure 6.21 indicate that the majority of the respondents agree with this statement (i.e. 56% strongly agree and 42% agree). Furthermore, Hill and Turbitt (2006) emphasised the importance of using both the organisational strategy as well as the IT strategy as input to define the IT security strategy. It is therefore safe to conclude that an IT security strategy should use the organisational strategy and the IT strategy as input elements.

6.2.4.2. Question 7(b): Section 4 of the questionnaire

The ITIL framework demonstrates the importance of considering previous incidents during the root cause analysis process in order to reduce recurring incidents (ITSMF, 2007). Adopting this principle in managing IT security risk will assist in ensuring that

during risk identification, previous risk and incidents are considered during the risk identification process.

The objective of incorporating this principle is to ensure that a comprehensive view of the IT security risk profile is accounted for and that the chances of previous risk materialising are minimised. Question 7(b) assessed the respondents' view' in considering previous risk and incidents during the IT security risk identification process. Figure 6.22 illustrates the response summary for question 7(b) of the questionnaire.

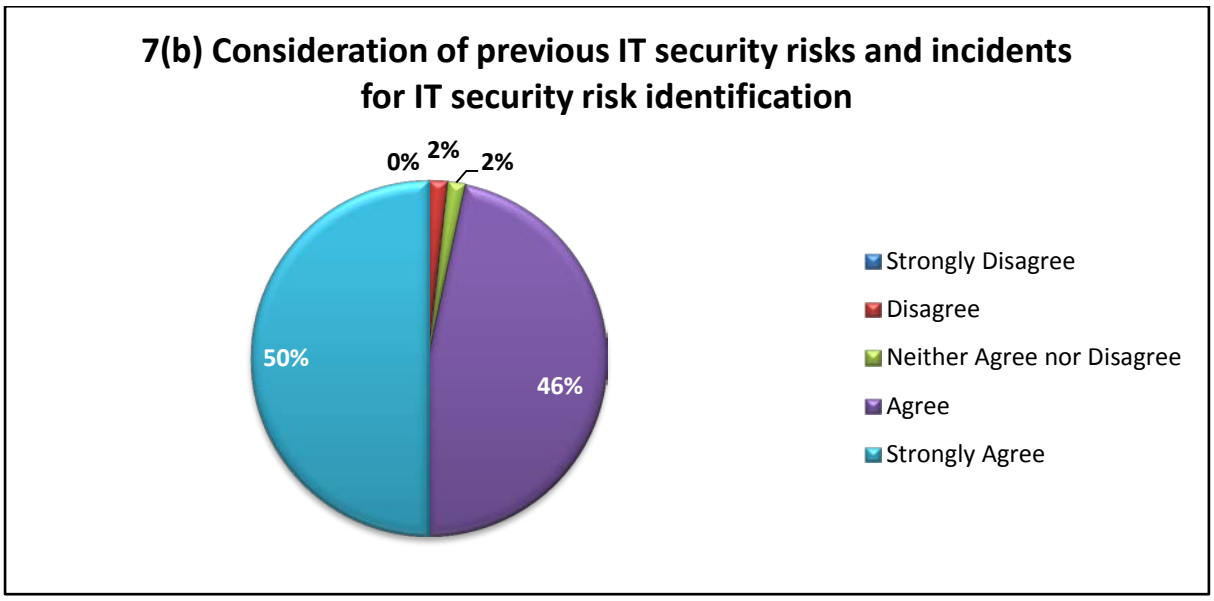

Figure 6.22 – Question 7(b): Consideration of previous IT Security Risks and Incidents

Figure 6.22 indicate that the majority of the respondents agree with the statement presented in question 7(b) (i.e. 46% of the respondents agree and 50% strongly agree). Only 2% of the respondents neither agree nor disagree with this statement, whereas the remaining 2% of them disagree. Based on the ITIL framework's recommendation and the high level of agreement by the respondents, this principle is considered a good principle for the ITSRB approach.

6.2.4.3. Question 7(c): Section 4 of the questionnaire

An audit finding is another source of risk (ITGI, 2007). Audit findings indicate the areas of IT security which have weaknesses in controls that may have been associated with a process, people or technology (ITGI, 2007). To ensure that all risk

is accounted for, it is important to consider audit findings for IT security during IT security risk identification. The objective of question 7(c) was to assess the respondents' views in considering IT security audit findings during the risk identification process. Figure 6.23 presents the response summary for question 7(c) of the questionnaire.

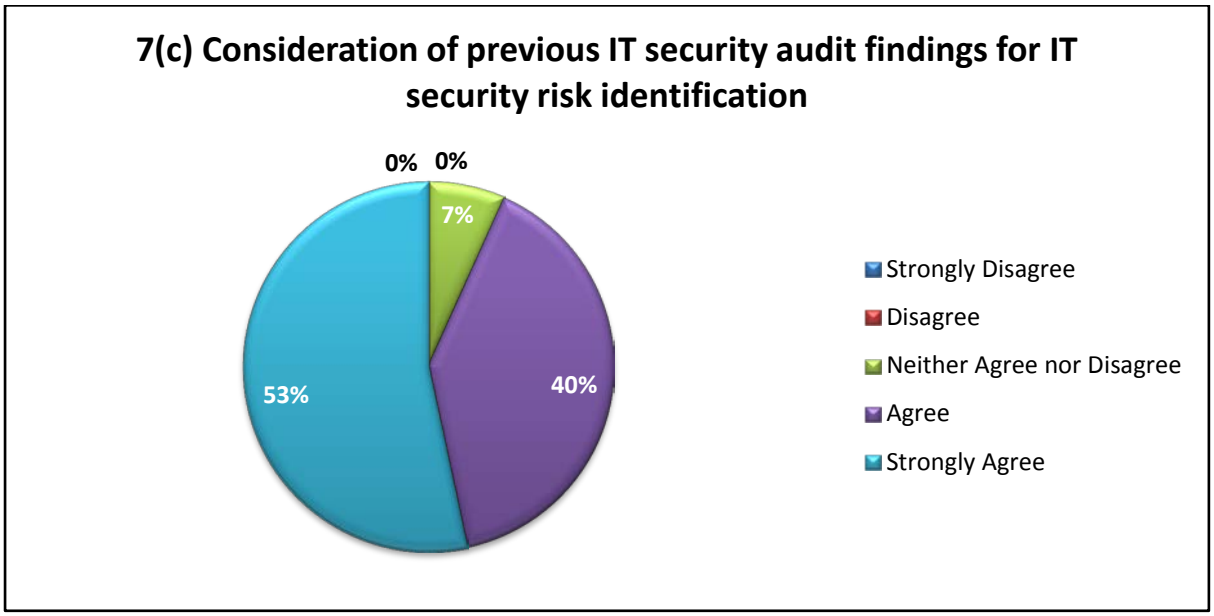

Figure 6.23 – Question 7(c): Consideration of IT security Audit Findings

From Figure 6.23, it is apparent that the minority of the respondents (i.e. 7%) neither agree nor disagree with this principle. However, the majority of the respondents agree with this principle (i.e. 40% agree and 53% strongly agree). Based on the fact that audit findings are another source of risk and the agreement level of the respondents, it is safe to make the deduction that considering IT security audit findings during the IT security risk identification process is essential.

6.2.4.4. Question 7(d): Section 4 of the questionnaire

One of the issues which remain unsolved in managing IT security risk includes the need of a formal risk management process for IT security (Krichene, 2008). The objective of question 7(d) was to assess the respondents' views about the formal assessment of IT security risk on a periodic basis to ensure that this risk is adequately managed. Figure 6.24 depicts the response summary for question 7(d) of the questionnaire.

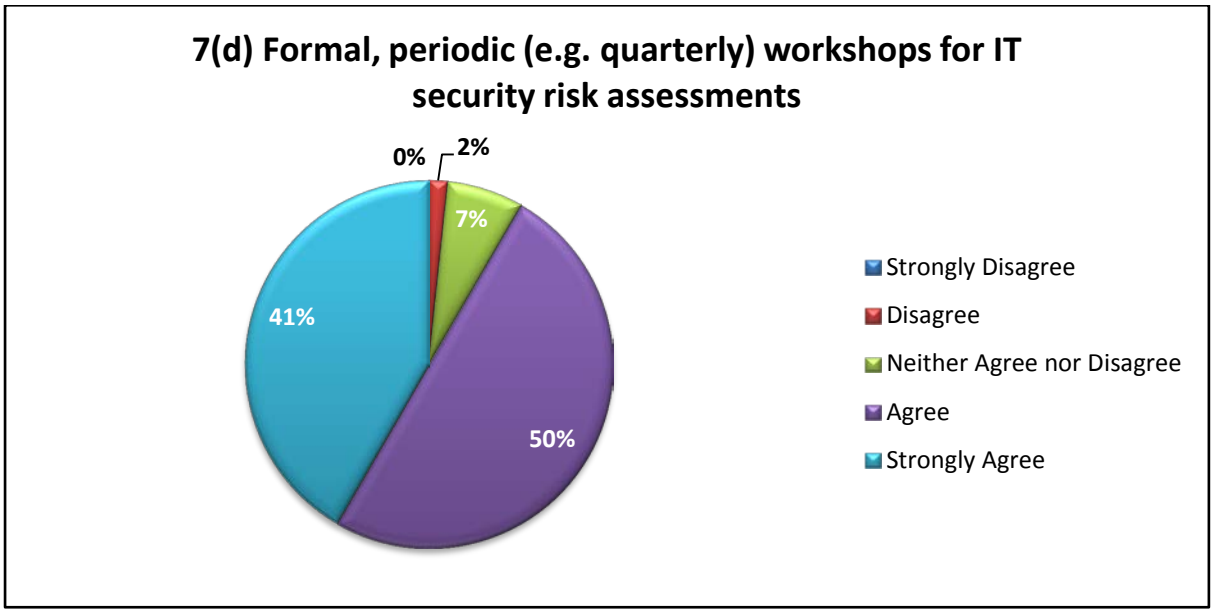

Figure 6.24 – Question 7(d): Periodic IT Security Risk Assessment

It is evident from Figure 6.24 that the majority of the respondents agree with this principle (i.e. 50% agree and 41% strongly agree). Seven per cent of the respondents neither agree nor disagree, while 2% of them disagree. As previously demonstrated in Chapter 3, many organisations have failed in managing the risk associated with IT security because IT security risk management is not formalised. It is therefore safe to make the conclusion that this principle is a good principle for the ITSRB approach.

6.2.4.5. Question 7(e): Section 4 of the questionnaire

The direction that any organisation follows is directed by its business operations (Hill & Turbitt, 2006). The type of business that is conducted by any organisation introduces specific IT security risk. It is therefore important to consider IT security threats that are facing a specific organisation in managing IT security risk to ensure that the correct risks are managed (Gandotra, et al., 2012). Question 7(e) assessed the respondents' views with regard to including threat modelling as part of the IT security risk management process. Figure 6.25 highlights the response summary for question 7(e) of the questionnaire.

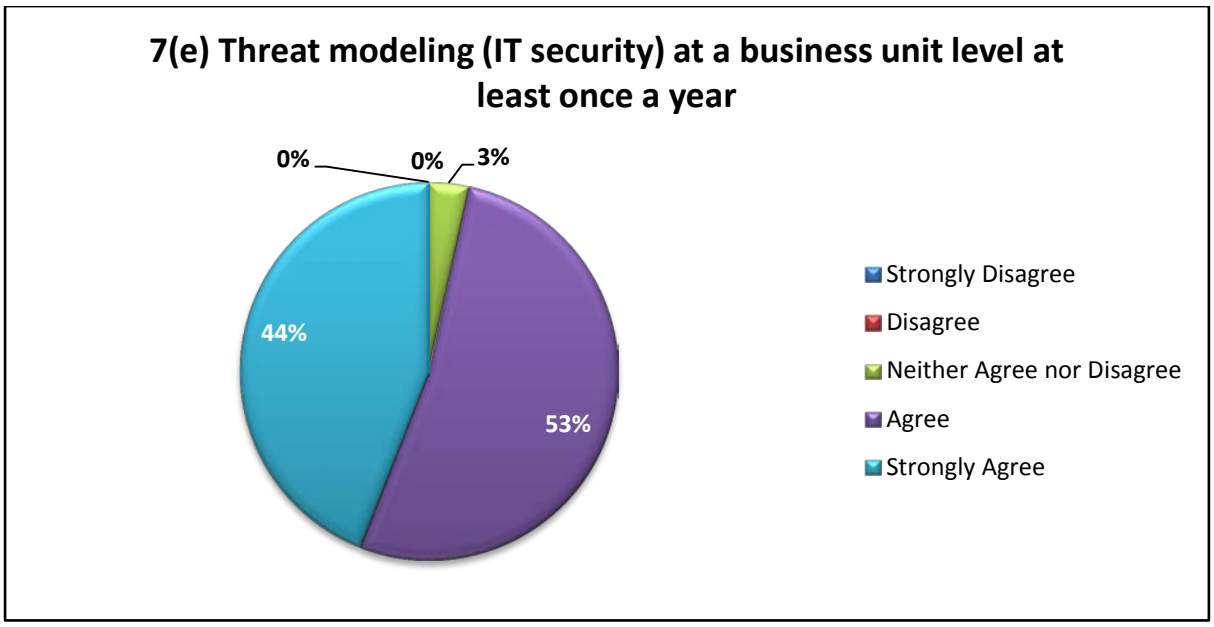

Figure 6.25 – Question 7(e): Threat Modelling

Figure 6.25 indicates that all respondents agree with this principle (i.e. 53% of the respondents agree and 44% strongly agree). It is therefore safe to conclude that including threat modelling as an integral part of an IT security risk management process is vital.

6.2.4.6. Question 7(f): Section 4 of the questionnaire

It is essential to ensure that all risk is documented to allow for knowledge sharing (Institute of Risk Management [IRM], 2010). Documenting and agreeing all risk elements assists in ensuring that important risk information is available and communicated as and when required to the relevant stakeholders (IRM, 2010). The first step in documenting risk is achieved through the use of a risk register that is reviewed regularly. Question 7(f) assessed the respondents' views on creating and maintaining an IT security register which is reviewed regularly. Figure 6.26 illustrates the response summary for question 7(f) of the questionnaire.

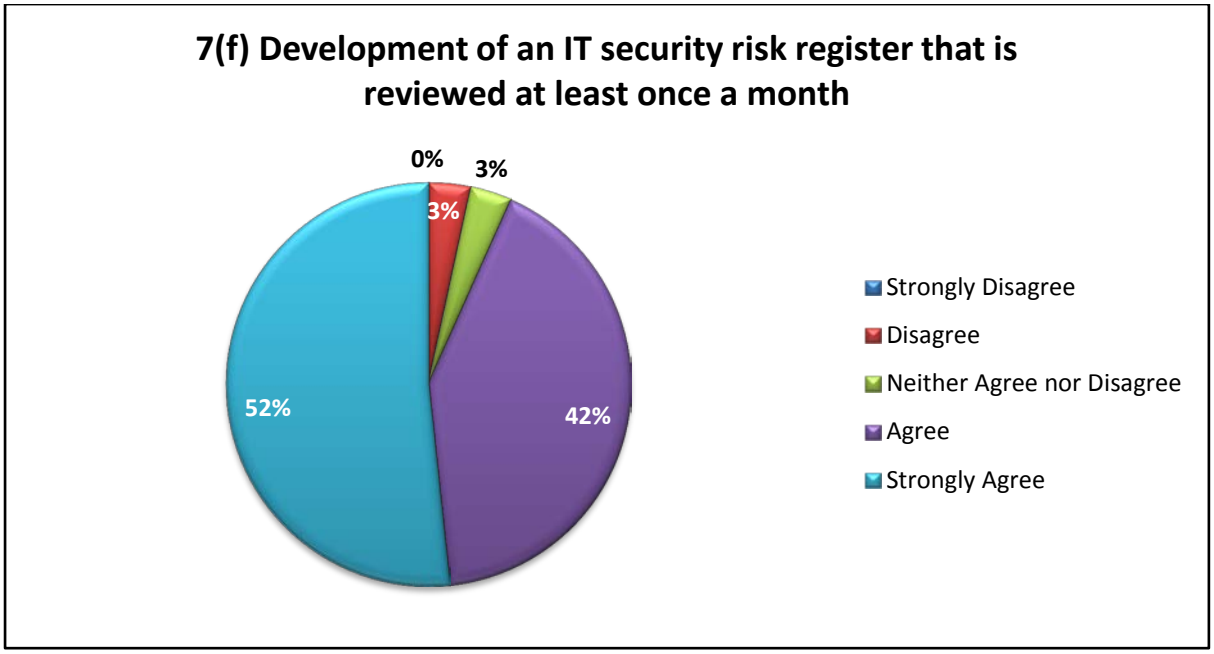

Figure 6.26 – Question 7(f): IT Security Risk Register

Figure 6.26 demonstrates that only 3% of the respondents disagree with this principle. The majority of the respondents agree (i.e. 42% agree and 52% strongly agree). Based on recommendations from IRM (2010) and the level of agreement of the respondents, it is safe to make the conclusion that this principle also provides a good base for the ITSRB approach.

6.2.4.7. Question 7(g): Section 4 of the questionnaire

Managing IT security risk is a process that involves an entire organisation, from senior management to most junior staff (NIST, 2010). Because senior management is ultimately accountable for risk management, progress of risk should be communicated to them on a periodic basis, including IT security risk (NIST, 2010). Communicating IT security risk formally will ensure that the IT risk profile and areas of improvement are known by the leadership of the organisation. The objective of this question was to assess the respondents' views about the importance of formally communicating the IT security risk profile on a periodic basis. Figure 6.27 depicts the response summary for question 7(g) of the questionnaire.

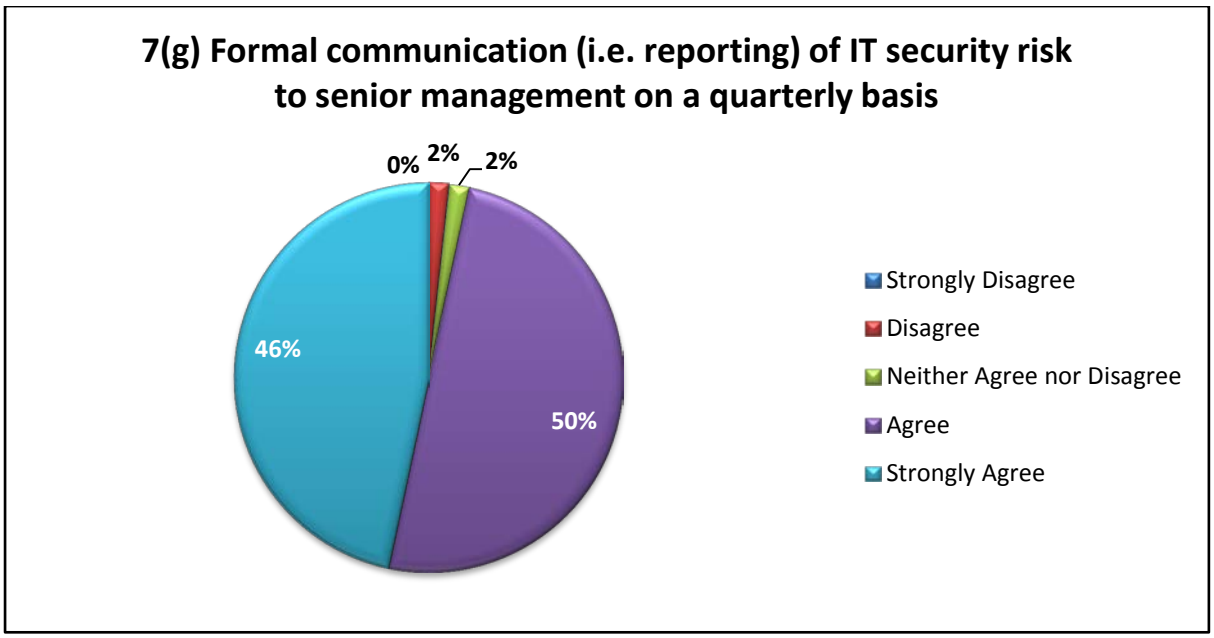

Figure 6.27 – Question 7(g): IT Security Risk Reporting

As indicated in Figure 6.27, all the respondents to this question agree with this principle (i.e. 50% agree and 46% strongly agree). It is therefore safe to assume that this principle is important to include as an integral part of the ITSRB approach.

6.2.4.8. Summary of section 4 responses

For all the principles presented in section 4 of the questionnaire, the results indicate agreement from the responses. The principles presented in this section have been used as integral components of the ITSRB approach. The agreement from the respondents therefore confirms that the principles applied to the ITSRB approach are crucial for effective management of IT security risk.

6.3. CONCLUSION

This chapter presented the results of the survey as well as the analysis of the findings for each section of the questionnaire. It is important to note that all the questions presented in the questionnaire were linked to the research objective and sub-objectives of this study, presented in Figure 2.4. The reason for linking the research objective to the questionnaire was to ensure that the questions asked to the respondents followed a sound approach. The questions used in the questionnaire assessed the elements, attributes and principles of the ITSRB approach, which were based on the IT security frameworks and standards, risk management principles and IT security threat modelling found in Chapter 4.

Throughout the questionnaire responses, the majority of the respondents agreed with the statements presented. Sporadically, there were negative responses from some of the respondents which highlighted disagreement with some of the presented statements. However, Chapters 3 and 4 provided a good source for some of the IT security frameworks and standards' principles. The conclusions made for each question from the questionnaire were not only made from a theoretical point of view but also considered the respondents' answers.

It is therefore safe to conclude that the ITSRB employs sound attributes and principles which can assist organisations in managing IT security risk better. The research objective and sub-objectives proposed in Chapter 1 were indeed satisfied with the results of this survey.

The final chapter concludes this study by summarising the discoveries made from conducting this study as well as proposing recommendations for future research.

7. CONCLUSION

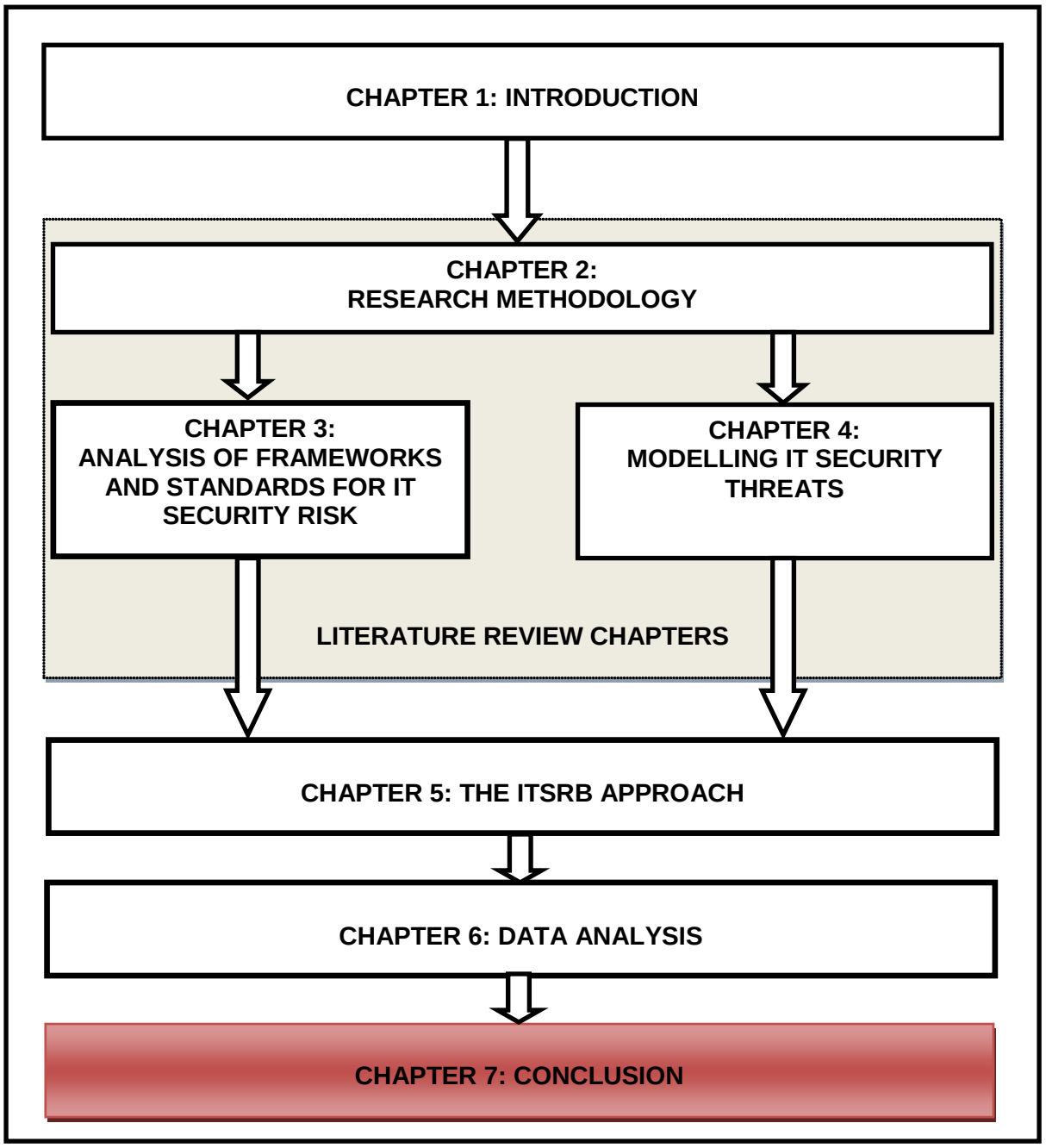

Figure 7.1 – Dissertation Layout: Chapter 7

7.1. INTRODUCTION

The main objective of this study is to investigate whether strong characteristics of the existing IT security frameworks and standards, the basic risk management principles, and the IT security threat modelling processes within the best practice body of knowledge can be extended to develop a formal and proactive approach to managing IT security risk. The main objective of this study is achieved through the development of the ITSRB approach, which is a new contribution made to the field of IT security.

The motivation for developing the ITSRB approach was pointed out during the literature review within the current body of knowledge, in chapter 1 of this study. Chapter 3 demonstrated that there are a number of IT security frameworks and standards that are available for use. However, there are still a number of challenges in the formalisation of IT security risk management, which this study proposed to address. The intention was to reuse the existing IT security frameworks and standards by extracting their strong characteristics, risk management principles and threat modelling to develop a unified approach that addresses the identified gaps.

The penultimate chapter analysed the data for this study. The purpose of this concluding chapter is to discuss the process that was followed in drawing the conclusions that were made. The research objective and the sub-objectives are reassessed to establish how they are achieved through the development of the ITSRB approach, in Section 7.2. Section 7.3 revisits the research questions that underpin the research objective and research sub-objectives, as presented in Chapter 1. The research questions are evaluated in order to ascertain how they meet the research objective of this study. Sections 7.4 and 7.5 present the strengths and the weaknesses of the ITSRB approach respectively. Section 7.6 deals with the weaknesses from the investigated IT security frameworks and standards addressed by the ITSRB approach. Section 7.7 provides recommendations for future work, followed by Section 7.8, which concludes the chapter and this study.

7.2. RESEARCH OBJECTIVE

Chapter 1 presented the research objective as follows:

To investigate whether strong characteristics of the existing IT security frameworks and standards, the basic risk management principles, and the IT security threat modelling processes within the best practice body of knowledge can be extended to develop a formal and proactive approach for managing IT security risk.

The main research question of this study was presented in Chapter 1 as follows:

Can a formal, dynamic and proactive approach for managing IT security risk be developed through the use of existing IT security frameworks and standards, basic risk management principles, and IT security threat modelling processes?

The above-mentioned research objective was achieved through answering the main research question and ultimately developing the ITSRB approach. The ITSRB approach embodied strong characteristics of the evaluated IT security frameworks and standards as a base. Thereafter, threat modelling was incorporated in order to increase the level of dynamicity of this approach. Lastly, basic risk management principles were incorporated to ensure that the ITSRB approach follows a robust process of managing IT security risk.

Additionally, the research methodology in this study was carried out in the form of a survey to evaluate the ITSRB approach. This was achieved by assessing the level of agreement from IT security experts within the scope of this study on the ITSRB approach. The survey yielded positive results as presented in Chapter 6.

7.3. RESEARCH SUB-OBJECTIVES

The study was based on three research sub-objectives and their supporting questions. The research sub-objectives coupled with their research questions – which were presented in Chapter 1 – are follows:

Research sub-objective 1: *Investigate the best practice IT security frameworks and standards which are most commonly used within the financial institutions in South Africa by identifying their common characteristics and limitations.*
Research question 1: *Do the selected best practice IT security frameworks and standards most commonly used within the financial institutions in South Africa assist in managing IT security risk?*

Research sub-objective 2: *Investigate basic risk management principles and IT security threat modelling processes to assess their benefits for IT security risk management.*
Research question 2: *Can best practice risk management principles and IT security threat modelling processes be adopted for IT security risk management?*

Research sub-objective 3: *Consolidate the strong characteristics of the investigated IT security frameworks and standards, basic risk management principles, and IT security threat modelling processes to develop characteristics and attributes of a dynamic IT security risk management approach.*
Research question 3: *Do the characteristics and attributes deduced from the investigated IT security frameworks and standards, risk management principles, and IT security threat modelling processes provide a good base for a proactive and dynamic IT security risk management approach?*

The three sections that follow discuss the manner in which the research questions are answered in this study.

7.3.1. Research sub-objective 1

As discussed in Chapter 3, there are many IT security frameworks and standards which exist in the current body of knowledge addressing various areas of IT security from encryption to application security, to data leakage, to compliance. Furthermore, because the scope of this study is limited to financial institutions within South Africa, the frameworks and standards chosen are amongst the well known and mostly used.

For the above reasons, the literature review section evaluated five IT security frameworks and standards, namely, OCTAVE, ISO 27001, COBIT, ITIL, and ISF

Standard of Good Practice. The frameworks and standards reviewed either solely focused on IT security (i.e. OCTAVE, ISO 27001/2 and ITIL) or have components that focus on IT security (i.e. COBIT and ITIL).

The detailed analyses of the frameworks and standards evaluated have similar objectives in respect of IT security, which is to safeguard the confidentiality, integrity and availability of information and/or systems. Moreover, these frameworks and standards provide a generic blueprint for managing IT security, resulting in better-managed risk as well as reduced vulnerabilities.

Research sub-objective 1 and the associated research question were answered through a detailed analysis of the evaluated frameworks and standards conducted in Chapter 3. In addition to that, section 2 of the questionnaire yielded positive results from the IT security professionals who participated in the survey. It is therefore safe to deduce that this research objective and the associated research question were achieved.

7.3.2. Research sub-objective 2

To achieve research sub-objective 2 as well as answer the associated research question, basic risk management principles and threat modelling processes were evaluated in Chapters 3 and 4 of this study respectively. In addition, to ensure that a risk based approach is incorporated, the ISO 31000 framework which provides the basic risk management principles was reviewed in Chapter 3. Incorporating the risk management principles in the management of IT security risk would ensure that the process is more formal and that risk is prioritised based on its criticality.

In addition to the foregoing, the threat modelling process was presented in Chapter 4 to demonstrate the importance of modelling IT security threats during IT security risk management. Threat modelling assists in ensuring that the correct focus is placed on the threats that face an organisation, thereby providing a dynamic process for IT security risk management.

In view of the aforementioned points, incorporating basic risk management principles and threat modelling process into an IT security risk management process was

deemed necessary. This research objective, as well as the associated research question, was further evaluated in section 3 of the questionnaire, which yielded positive results. For this reason, it is safe to conclude that this research objective was achieved.

7.3.3. Research sub-objective 3

Concerning research sub-objective 3 and its accompanying research question, the comparative analysis conducted and presented in Chapter 5 indicated that frameworks and standards generally tend to focus on a specific level of management, thus creating gaps. Because of this, some IT security risks may be missed because of the applicability level of the frameworks and standards.

Furthermore, the analysis conducted revealed that the majority of the investigated IT security frameworks and standards (i.e. COBIT 4.1, ISO 27001, ITIL, and ISF SoGP) focus on recommending security controls and not providing recommendations for prioritising these controls. Organisations may easily find themselves chasing the implementing of security controls, not taking into account the risk that faces them.

Consolidating the IT security frameworks and standards' strong characteristics, threat modelling and risk management principles was found to be necessary for providing an approach that is comprehensive, dynamic and proactive in managing IT security risk. Furthermore, the principles of the ITSRB approach were evaluated through section 4 of the questionnaire by IT security professionals who participated in the survey. The survey yielded positive results from the majority of the respondents. Additional validation was received on the ITSRB approach (i.e. in Chapter 5), as it was accepted at the International Conference Information Security for South Africa 2015, where valuable feedback and comments were attained and incorporated. The next section discusses the strengths of the ITSRB approach.

7.4. STRENGTHS OF THE ITSRB APPROACH

The motivation for this study (presented in Chapter 1) highlights the gaps that are encountered in managing IT security risk. The ITSRB approach bridges the identified gaps by incorporating the elements that follow as a base.

7.4.4. Basic risk management principles

The ITSRB approach incorporates the ISO 31000 risk management principles in identifying, assessing, treating and communicating IT security risk. This ensures that a robust and iterative process is followed in managing IT security risk management, thereby ensuring that IT security risk is managed alongside with other organisational risks.

Furthermore, the ITSRB approach provides a mechanism that ensures that IT security risk is managed holistically throughout all levels of management (i.e. strategic, tactical and operational level). In this way, IT security risk receives the correct level of attention within any organisation.

7.4.5. Proactive and dynamic approach

The ITSRB approach incorporates threat modelling to manage IT security risk. As previously discussed in the literature review section, IT is dynamic in nature, making the threats that arise from this environment dynamic as well. Proactively identifying threats and taking them into account during risk management provides a solution that actively addresses the risks that matter.

7.4.6. Consolidated characteristics of best practice frameworks and standards

The ITSRB uses consolidated characteristics of the best practice frameworks and standards as a base. As demonstrated in the literature review, some frameworks and standards lack in certain aspects and are strong in other regards. Consolidating the strong characteristics provides an approach that is comprehensive and more effective.

7.4.7. Involvement of the entire organisation

The ITSRB approach follows a consultative process which involves all levels of management within the organisation. In this way, a comprehensive view of the IT security risk profile is gathered about an organisation, reducing the risk of failing to identify other IT security risks that may be left out because of misplaced focus.

Complete elimination and mitigation of any risk is impossible; consequently, the ITSRB approach may have some weaknesses which are unknown. Section 7.7 discusses the weaknesses identified for the ITSRB approach.

7.5. WEAKNESSES OF THE ITSRB APPROACH

It is important to acknowledge that no framework is perfect, as there is an overwhelming amount of information available that cannot be addressed. The weaknesses that follow were identified for the ITSRB approach.

7.5.1. Scope of the study

The scope of this study was limited to a specific industry (i.e. financial institutions within South Africa). For this reason, the ITSRB approach may have shortfalls when applied to other industries (such as telecommunications and health). There are other IT security frameworks and standards which are equally good or better within the field of IT security. The information used to define the ITSRB approach was only limited to frameworks and standards which were studied in detail.

7.5.2. Theoretical base

The ITSRB approach has not been tested in a real-world situation but is based on existing literature and studies. For this reason, the assumptions made about its effectiveness are interpretative. Subsequently, the results achieved from the research methodology carried out are based on the interpretation of the existing literature and may often be subjective in the natural sense.

7.5.3. Limitation of the survey

As previously discussed, a survey was carried out as the research methodology for this study. The survey was quantitative in nature and therefore did not provide a flexible mechanism that allowed the respondents to provide reasons for selecting the answers they chose. As a consequence, in instances where respondents did not agree with the presented statements, it is not possible to know why. Knowing this

information would have provided the data analysis section with more value, thereby identifying more areas of weaknesses for the ITSRB approach.

Furthermore, with the chosen research methodology, it is always best to have as many respondents as possible. It is acknowledged that even though the sample size was small and provided an acceptable confidence level, a higher response level would have provided a better confidence level (i.e. 95% or higher).

7.6. DEFICIENCIES FROM THE INVESTIGATED FRAMEWORKS AND STANDARDS ADDRESSED BY THE ITSRB APPROACH

It was demonstrated in Table 5.1 that the selected frameworks and standards have different shortcomings, some of which are addressed by the ITSRB approach. At a high level, the ITSRB approach addresses the following aspects:

- **Organisational-wide view** (Webb, Ahmad, Maynard & Shanks, 2014): Attribute 1, discussed in Chapter 5, ensures that a comprehensive view of the IT security risk profile is captured within an organisation from the operational level up to the strategic level.
- **Slow response and reactiveness** (Utin, Utin & Utin, 2008): Attribute 2 and attribute 5, discussed in Chapter 5, emphasises the importance of threat modelling which ensures that new threats are iteratively considered to ensure that a risk based approach is followed. This enables organisations to be more proactive.
- **Accountability** (Nastase, et al., 2009): Attribute 3, discussed in Chapter 5, emphasises the need for explicitly documenting responsibilities when processes are executed.
- **Knowledge management** (Shedden, Scheepers, Smith & Ahmad, 2011): The ITSRB approach emphasises the importance of capturing tacit knowledge in the risk management process to ensure continuity in the process. This is demonstrated in all the phases of the ITSRB approach presented in Chapter 5.

7.7. FUTURE WORK

In recommending future work for this study, the weaknesses of the ITSRB approach discussed in section 7.5 of this chapter were considered. The following areas would add more value in the IT security field if further research is conducted:

- The study can be expanded beyond the financial institutions of South Africa. Financial institutions in other countries may be doing things differently compared to those in South Africa (e.g. better operational processes inherently reducing IT security risk, and better technologies introducing more IT security risk).

- The study can be expanded beyond the financial institution industry. There are other industries such as telecommunications, health, manufacturing, and aviation that can benefit from the use of a similar approach. Furthermore, it would be interesting to determine if the ITSRB approach is over- or under-engineered for other industries.

- Because the ITSRB approach was defined using only five best practice frameworks and standards, it might be limited in other aspects. Investigation of other best practice IT security frameworks and standards can also provide more value in enhancing the ITSRB approach. The tools that were recommended for the ITSRB approach may also have shortfalls which may be addressed by other tools if further investigation is pursued.

- Implementing the ITSRB approach using empirical research methods (e.g. action research) would add more value by demonstrating the actual value or shortcomings when this approach is put into practice within a real organisation. This study was conducted based on theoretical assumptions and observations.

7.8. CONCLUSION

This section reflects on the process that was followed to develop the ITSRB approach. The motivation for this study, discussed in chapter 1 of this study, proved to be viable as it provided current concerns which exist within different organisations in managing IT security risk. To determine a robust methodology for conducting this

study, chapter 2 investigated the most suitable research methodology which would provide the optimal results used to conclude this study.

Based on the fact that there are frameworks and standards for IT security in the existing literature, it was deemed necessary to adopt and reuse some of the key principles from those frameworks and standards to develop the ITSRB approach. The selected frameworks and standards for IT security were investigated and discussed in detail within chapter 3 of this study.

IT security is a dynamic discipline, what is valid today may not be valid tomorrow. For this fact, a formal process for threat modelling was investigated and discussed in chapter 4 to ensure that the constant changes that face the discipline of IT security are taken into consideration while developing the ITSRB approach.

The ITSRB approach was developed and presented in chapter 5 of this study, using the theoretical foundation discovered in the previous chapter (i.e. chapters 1 - 4). At this point, a questionnaire was sent out to IT security professionals whereby the principles and attributes of the ITSRB approach were independently evaluated. Chapter 6 analysed the results from the respondents, which indicated that majority of the respondents were in agreement with how the ITSRB approach was constructed.

Furthermore, the ITSRB approach was presented in a peer reviewed academic conference (Information Security South Africa - 2015) to validate its effectiveness and robustness. The feedback received from the IT security professionals who attended the conference was positive and viable. Constructive feedback received from the conference was used to enhance the final ITSRB approach presented in this study.

Having reflected on the process followed to develop the ITSRB approach, it is safe to conclude that the ITSRB approach enhances the way IT security risk is managed within organisations thereby providing a blueprint for IT security risk management. This does not take away the fact that it is subject to being improved by peers to enhance the challenges that generally face IT security professionals within various industries. Combining efforts and ideas will help the ITSRB approach to becoming an

optimal solution that assists individuals and organisations in managing this type of risk.

In concluding this study, this quote below is highlighted: *“What you do today, may improve all your tomorrows” ~ Ralph Marston.* In the same vein, the ITSRB approach is a blueprint that can be used in improving the manner in which IT security is managed, thereby enhancing the future of IT security risk management.

REFERENCES

Adèr, H., Mellenbergh, G. & Hand, D., 2008. *Advising on research methods: A consultant's companion..* Huizen: Johannes_van_Kessel.

Ajibuwa, F., 2008. *Data and Information Security in Morden day Businesses. ,* s.l.: Atlantic International University.

Albert, C. & Dorofee, A., 2001. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Criteria Version 2.0,* s.l.: Software Engineering Institute: CMU/SEI-2001-TR-016.

Alberts, C., Dorofee, A., Stevens, J. & Woody, C., 2003. *Introduction to the OCTAVE® Approach, Networked Systems Survivability Program,* Pittsburgh: Software Engineering Institute(PA 15213-3890).

Alhabeeb, M., Almuhaideb, A., Dung, P. & Srinivasan, B., 2010. *Information Security Threats Classification Pyramid.* Melbourne Australia, IEEE 24th International Conference on Advanced Information Network.

Amoroso, E., 1994. *Fundamentals of Computer Security Technology.* NJ: Prentice-Hall PTR - Upper Saddle River.

Amsenga, J., 2005. An Introduction to Standards Related to Information Security. *An Introduction to Standards Related to Information Security*.

Anon., n.d. *108. Security Innovation. Threat Modeling Methodology. Visualizing and mitigating software risk..* [Online] Available at: www.securityinnovation.com [Accessed 12 February 2013].

Antonius, R., 2003. Interpreting Quantitative Data with SPSS. In: London: SAGE, pp. 127-136.

Arora, A. et al., 2004. Measuring the risk-based value of IT security solutions. *IT Professional,* 6(6), pp. 35 - 42.

Arveson, P., 2015. *The Deming Cycle - PDCA Model.* [Online] Available at: www.balancedscorecard.org [Accessed 20 February 2016].

Banacorsi, S., 2011. *What is a RACI ,* s.l.: 6sixsigma.

Bandyopadhyay, K., Myktyn, P. & Myktyn, K., 1999. A framework for integrated risk management in information technology. In: Emerald, ed. *Management Decision.* USA: MCB UP Ltd, pp. 437 - 445.

Barribeau, P. et al., 2005. *Survey research,* Colorado: Colorado State University Department of English.

BCBS, 2006. Basel Committee on Banking Supervision . In: B. f. InternationalSettlements, ed. *Basel II: International convergence of capital measurement and capital standards: A revised framework-comprehensive version.* s.l.:BCBS Publications.

Belli, G., 2008. *Non-experimental quantitative research.* Lapan: Wiley.

Berg, B., 2004. Qualitative research methods for the social sciences. In: BaconandAllyn, ed. *Qualitative research methods.* 5 ed. New York: Pearson, pp. 44-65.

Bharadwaj, A., 2002. *Integrating Positivist and Interpretive Approaches to Information Systems Research,* s.l.: A Lakatosian Model.

Bhasker, R. & Kapoor, B., 2009. Information Technology Security Management. In: *Computer and Information Security Handbook.* s.l.:s.n., pp. 259-267.

Bishop, M., 2005. *Introuction to Computer Security.* 1 ed. Boston: Addison Wesley.

Bradley, R. & Pratt, R., 2011. *Exploring the Relationships Among Corporate Entrepreneurship, IT Governance, and Risk Management.* Hawaii, IEEE.

Brill, J., 2008. Likert Scale: Encyclopedia of Survey Research Methods. In: T. Oaks, ed. CA: SAGE Research Methods Online, pp. 428-430.

Bryman, A. & Cramer, D., 2001. Quantitative data analysis with SPSS Release 10 for Windows: . In: *A guide for social scientists.* Hove: Routledge, pp. 12-29.

Burns, S., 2005. *Threat Modeling: A Process To Ensure Application Security. ,* s.l.: SANS Institute: InfoSec Reading Room.

Calder, A., 2013. *, "Information Security and ISO 27001:An Introduction, IT Governance Green Paper: Infosec-and-ISO27001v3,* London, UK: s.n.

Calder, A., 2013. *Information Security and ISO 27001: An Introduction,* UK: IT Governance Green Paper:Infosec-and-ISO27001v3.

Chaplin, M. & Creasy, J., 2011. *The ISF Standard of Good Practice,* London: Information Security Forum (ISF) Limited. .

Cheney, J. & Furner, K., 2008. *HP Project and Portfolio Management Center Briefing,* USA: Hewlett-Packard Development Company.

Chen, S. et al., 2003. *Modeling and evaluating the security threats of transient errors in firewall software. Center for Reliable and High-Performance Computing,* USA: Elsevier.

Chisnall, M., 1997. Marketing Research. In: 5th edition ed. UK: McGraw-Hill Publishing, pp. 76-89.

Chorppath, A. & Alpcan, T., 2012 . *Risk Management for IT Security: When Theory Meets Practice.* Istanbul , IEEE .

Chowdhury, M., Matulevičius, R., Sindre, G. & Karpati, P., 2012. *Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions,* Berlin: Springer-Verlag .

Chowdhury, M., Matulevičius, R., Sindre, G. & Karpati, P., 2012. *Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions.* Berlin, Springer-Verlag.

Cobanoglu, C., Warde, B. & Moreo, P., 2001. A comparison of mail, fax and Web-based survey methods. In: B. S. C. A. 5540849, ed. *International Journal of Market Research.* s.l.:EBSCOHost, pp. 43:441-452.

Commission, C. o. S. O. o. t. T., 2015. *The Committee of Sponsoring Organizations of the Treadway Commission.* [Online] Available at: www.coso.org [Accessed 1 February 2013].

COSO, 1985. *The Committee of Sponsoring Organizations of the Treadway Commission.* [Online] Available at: www.coso.org [Accessed 1 February 2013].

Dawson, C., 2002. *Practical Research Methods.* New Delhi: UBS Publishers Distributors.

Ding, C. & Behera, R., 2009. *Enterprise Risk and Governance Trends, Vendors, and Market Outlook,* USA: Celent Research.

Dubois, E., Heymans, P., Mayer, N. & Matulevičius, R., 2010. A Systematic Approach to Define the Domain of Information System Security Risk Management. A systematic approach to define the domain of information system security risk management. In: *International Perspectives on Information Systems Engineering.* Heidelberg: Springer, pp. 289-306.

Dykema, J., Blixit, S. & Stevenson, J., 2008. Ordinal Measure: Encyclopedia of Survey Research Methods. In: T. Oaks, ed. CA: SAGE, pp. 422-424.

Eaton, J. & Struthers, C., 2002. Using the Internet for organizational research: A study of cynicism in the workplace.. In: EBSCOHost, ed. *Cyber Psychology & Behaviour.* s.l.:Business Source Complete: AN 7303525, pp. 5:305-313.

ENISA, 2005. *European Union Agency for Network and Information Security.* [Online]
Available at: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-manage
[Accessed 20 February 2014].

Erasmus, J. & Breier, M., 2009. *Skills Shortages in South Africa: Case Studies of Key Professionals. South African Department of Labour..* ISBN (pdf) 978-0-7969-2273 ed. Pretoria: Human Science Research Council.

Farahmand, F., Navathe, S., Sharp, G. & Enslow, P., 2005. *A Management Perspective on Risk of Security Threats to Information Systems, ,* s.l.: Information Technology and Management archive.

Felegyhazi, M., 20011. *IT Risk Management – Economics of Security and Privacy,* s.l.: BME Department of Telecommunications - CrySysLab.

Felegyhazi, M., 2011. *IT Risk Management – Economics of Security and Privacy,* s.l.: BME Department of Telecommunications.

Fenz, S. & Ekelhart, A., 2009. *Formalizing Information Security Knowledge.* Sydney: ASIACCS'09.

Finne, T., 1996. *The Information Security Chain in a Company,* Finland: Finland University: Institute for Advanced Management Research.

Foley, S., 2009. *Security Risk Management using Internal Controls.* Ireland, WISG'09.

Fricker, R. & Schonlau, M., 2002. *Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature.* London: SAGE.

Gandotra, V., Singhal, A. & Bedi, P., 2012. *Threat-Oriented Security Framework: A Proactive Approach in Threat Management,* India: Elsevier.

Gartner, 2012. *Update in COBIT 5: Aim for Greater Relevance to Wider Business Audience Analysis,* s.l.: Gartner.

Geric, S. & Hutinski, Z., 2007. Information System Security Threats Classifications. *Journal of Information and Organizational Sciences,* Volume 31, p. 51.

Gershkoff, A., 2008. Level of Measurement. Encyclopedia of Survey Research Methods. In: T. Oaks, ed. CA: SAGE, pp. 556-557.

Gibson, M., 2012. *Critical Success Factors for the Implementation of an Operational Risk Management System for South African Financial Services Organisations,* Pretoria: University of Pretoria.

Griffis, S., Goldsby, T. & Cooper, M., 2003. Web-based and mail surveys: A comparison of response, data, and cost. In: B. S. C. A. 12067895, ed. *Journal of Business Logistics.* s.l.:EBSCOHost, pp. 24:237-258.

Hardy, G., 2012. *Beyond Continuous Monitoring: Threat Modeling for Real-time Response,* s.l.: SANS Institute: InfoSec Reading Room.

Heffner, C., 2004. *Research methods for education, psychology, and the social sciences ,* s.l.: s.n.

Hill, P. & Turbitt, K., 2006. *Combine ITIL and COBIT to Meet Business Challenges,* s.l.: BMC Software.

Howard, J., 1998. *1998. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation,* USA: Carnegie Mellon University Pittsburgh.

Howell J., P. M. et al., 2005. *Reliability and validity. Writing@CSU..* Colorado: Colorado State University Department of English.

Hutt, M. & Speh, T., 2001. *Business marketing management: A strategic view of industrial and organizational markets.* 7th ed. Fort Worth: Dryden Press.

Institute, I. G., 2008a. *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, 2008a,* USA: IT Governance Institute.

IOD, 2009. *KING III Code of Governance,* South Africa: Institute of Directors .

ISO/IEC13335, 2004. Part Concepts and models for information and communications technology security management. In: *Information Technology Security Techniques: Management of Information and Communications Technology Security.* s.l.:International Standard Organisation.

ISO/IEC, 2005. *International Standard for Information Security,* s.l.: International Standards Organisation.

ISO/IEC27001, 2007. *International Standard for Information Security,* s.l.: International Standards Organisation.

ISO/IEC27001, 2013. *International Standard for Information Security,* s.l.: International Standards Organisation.

ISO/IEC27005, 2005. *Information technology — Security techniques — Code of practice for information security management.,* s.l.: International Standards Organisation.

ISO/IEC31001, 2009. *Risk management -- Principles and guidelines,* s.l.: Internationl Standards Organisation.

ITGI, 2007a. *Cobit 4.1,* USA: IT Governance Institute.

ITGI, 2007. *Cobit 4.1,* USA: IT Governance Institute.

ITGI, 2007. *Framework-Control Objectives- Management Guidelines – Maturity Models,* USA: The IT Governance Institute.

ITGI, 2008b. *Cobit Mapping: Mapping of ITIL v3 With Cobit 4.1,* USA: IT Governance Institute 2008b.

ITGI, 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT,* USA: The IT Governance Institute.

ITSMF, 2007. *An Introductory Overview of ITIL V3 (version 1.0),* UK: The IT Service Management Forum.

Jahankhani, H. & Nkhoma, M., 2009. *Information Systems Security and Its Affiliation to Information Technology Risk Management,* Berlin Heidelberg: Springer-Verlag .

Jouini, M., Rabai, L. & Aissa, A., 2014. *Classification of security threats in information systems,* 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014): Elsevier.

Kalain, S., 2008. *Research Design - Encyclopedia of Survey Research Methods.* CA: SAGE.

Kaplan, R. & Saccuzzo, D., 2001. Psychological testing: Principles, applications, and issues. In: Belmont: Wadsworth, pp. 176-188.

Ketel, M., 2008. *IT security Risk Management.* s.l., ACM SE'08.

Ketel, M., 2008. *IT Security Risk Management,* s.l.: ACM-SE'08.

Kipling, R., 1902. *Just so stories..* 1st ed. s.l.:Double Day Page.

Klemen, M. & Biffl, S., 2004. *Economic Aspects and Needs in IT-Security Risk Management for SMEs. Institute of Software Technology and Interactive Systems,* Austria: Vienna University of Technology.

Knapp, T., 2008. Validity: Encyclopedia of Survey Research Methods. In: T. Oaks, ed. CA: SAGE, pp. 939-940.

Kolias, C. et al., 2016. Learning Internet-of-things Security "Hands On". *IEEE Security & Privacy,* 14(1), pp. 37 - 46.

Kothari, C., 1985. *Research Methodology- Methods and Techniques..* New Delhi: Wiley Eastern Limited.

KPMG, 2009. *King III report.* [Online] Available at: http://www.kpmg.com [Accessed 25 October 2012].

Krauss, S., 2005. *Research Paradigms and Meaning Making: A Primer,* s.l.: The Qualitative Report.

Krichene, J., 2008. *Managing Security Projects in Telecommunication Networks,* s.l.: SUP'COM - Engineering School of Communications.

Langner, R., 2013. *The RIPE Framework: A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security ,* s.l.: Langner Communications White Paper.

LeBlanc, H., 2003. *Writing Secure Code.* 2nd ed. Redmond Washington: Microsoft Press.

Lewis, E. & Millar, G., 2009. *The Viable Governance Model – A Theoretical Model for the Governance of IT.* Hawaii, Proceedings of the 42nd Hawaii International Conference on System Sciences.

Lindqvist, U. & Jonsson, E., 1997. *How to systematically classify computer security intrusions,* s.l.: IEEE Symposium on Security and Privacy.

Maphakela, R., 2008. *A Model for Legal Compliance in the South African Banking Sector - An Information Security Perspective,* South Africa: Nelson Mandela Metropolitan University: Department of Information Technology.

Marek, P. & Paulina, J., 2006. The OCTAVE methodology as a risk analysis tool for business resources. In: ISSN:1896-7094, ed. s.l.:Proceedings of the International Multiconference on Computer Science and Information Technology, p. 485 – 497.

Mayer, N., 2009. *Model Based Management of Information System Security Risk,* s.l.: University of Namur.

Meier, J. et al., 2003. Chapter 3 - Threat Modeling. In: *Improving Web Application Security: Threats and Countermeasures .* Redmond: Microsoft Corporation.

Meier, J. et al., 2003. *Improving Web Application Security: Threats and Countermeasures,* s.l.: s.n.

Mohamed, S., Ribiere, V., O'Sullivan, K. & Mohamed, K., 2008. The Re-Structuring of the Information Technology Infrastructure Library (ITIL) Implementation using knowledge management framework. *The Journal of Information and Knowledge Management Systems,* 38(3), pp. 315-333.

Mougouei, D., Moghtadaei, M. & Moradmand, S., 2012. *A Goal-Based Modeling Approach to Develop Security Requirements of Fault Tolerant Security-Critical Systems. International Conference on Computer and Communication Engineering (ICCCE 2012),* Malaysia: IEEE.

Myagmar, S., Lee, A. & Yurcik, W., 2005. *Threat Modeling as a Basis for Security Requirements,* Urbana-Champaign: University of Illinois - National Center for Supercomputing Applications.

Myers, M., 2004. *Qualitative Research in Information Systems,* NZ: Staff Business Auckland.

Myers, M., 2011. *Qualitative Research in Information Systems,* s.l.: MIS Quarterly 21(2).

Myers, M. & Avison, D., 2002. *Qualitative Research in Information System,* London: SAGE.

Myers, M. & Klein, H., 2011. *A Set of Principles for Conducting Critical Research in Information Systems,* s.l.: MIS Quarterly 35(1).

Nair, M., 2009. *What is the difference between Framework and Standard,* s.l.: s.n.

Nakrem, A., 2007. *Managing Information Security in Organizations – A Case Study,* s.l.: Agder University College.

Nastase, P., Nastase, F. & Ionescu, C., 2009. *Challenges generated by the implementation of the IT Standards ITGI, ITIL V3 and ISO/IEC 27002 in enterprises.* s.l.:The Bucharest Academy of Economic Studies.

Netland, L., 2008. *Assessing and Mitigating Risks in Computer Systems. ,* Norway: University of Bergen.

NIST, 2004. *An Introduction to Computer Security: The NIST Handbook - Common Threats.* USA: National Institute of Standards and Technology Special Publication 800-12.

NIST, 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach,* Computer Security Division, Information Technology Laboratory: National Institute of Standards and Technology (NIST) Special Publication 800-37.

Oates, B. J., 2006. *Researchgin Information systesm and computing.* London: Sage Publications.

Oates, B. J., 2006. *Researching Information Systems and Computing.* 1st ed. s.l.:SAGE.

Obradovic, G., 2003. *Threat Modeling and Data Sensitivity Classification for Information Security Risk Analysis,* s.l.: Presentation at Data Protection'03.

Obrand, L., Augustsson, N., Holmstrom, J. & Mathiassen, L., 2012. *The Emergence of Information Infrastructure Risk Management in IT Services.* Hawaii, IEEE.

Ogut, H., 2006. *Information Technology Security Risk Management,* Dallas: The University of Texas.

OWASP, 2015. *Application Threat Modeling - OWASP.* [Online] Available at: https://www.owasp.org [Accessed 20 January 2015].

Panda, P., 2009. The OCTAVE Approach to Information Security Risk Assessment,. *ISACA Journal,* Volume 4.

Pelnekar, C., 2011. Planning for and Implementing ISO 27001. *ISACA JOURNAL,* Volume 4.

Penwarden, R., 2014. *Response Rate Statistics for Online Surveys -What Numbers Should You be Aiming For?,* s.l.: Fluid Surveys University.

Perkins, G., 2004. Will libraries' Web-based survey methods replace existing non-electronic survey methods? . In: EBSCOHost, ed. s.l.:Information Technology and Libraries, pp. 23(3): 123-126.

Ponenti, A., 2008. *An Integrative Risk Management/Governance Framework for Homeland Security Decision Making,* Carlifonia Monterey: Naval Postgraduate School.

Poolsappasit, N., 2010. *Towards An Efficient Vulnerability Analysis Methodology for Better Security Risk Management,* Colorado: Colorado State University.

Porteous, B. & Pradip, T., 2006. *Economic Capital and Financial Risk Management for Financial Services Firms and Conglomerates.* s.l.:Palgrave Macmillan: ISBN 1-4039-3608-0.

PSIRA, 2014. *Private Security Industry Regulatory Authority - Annual Report 2013 - 2014,* Pretoria: PSIRA.

PWC, 2009. *Executive Guide to King III.* [Online] Available at: www.pwc.co.za [Accessed 28 October 2012].

Q, Q. Y. & Chang, A., 2007. *Threats and countermeasures for information system security: A cross-industry study,* s.l.: Elsevier.

Rajasekar, S., Philominathan, P. & Chinnathambi, V., 2013. *Research Methodology,* India: Bharathidasan University-School of Physics.

Reid, R. & Gilbert, A., 2007. *Managing Security from the Perspective of the Business Executive.* New York, USA, ACM.

Risk_Management, I., 2010. *Institute of Risk Management: A structured approach to enterprise risk management,* London: The Public Risk Management Association.

Roos, J., 2008. *Residual Risk Management: A quantitative approach to Information Security.* Netherlands: University of Twente.

Rot, A. & Sobinska, M., 2013. *IT Security Threats in Cloud Computing Sourcing Model. Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 1153–1156..* s.l., IEEE.

Roztocki, N. & Lahri, N., 2003. *Is the applicability of Web-based surveys for academic research limited to the field of information technology?.* Hawaii, IEEE: HICSS'03 - Proceedings of the 36th Hawaii International Conference on System Sciences.

Saleh, M. & Alfantookh, A., 2011. A New Comprehensive Framework for Enterprise information Security Risk Management. *Applied Computing and Informatics,* Volume 9, pp. 107-118.

Schechter, S., 2004. *Computer Security Strength & Risk: A Quantitative Approach,* Massachusetts: Harvard University Cambridge.

Schneier, B., 2000. *Secrets & Lies..* s.l.:John Wiley & Sons, Inc..

Shedden, P., Scheepers, R., Smith, W. & Ahmad, A., 2011. Incorporating a knowledge perspective into security risk assessments. *VINE,* 41(2), pp. 152-166.

Sheehan, K., 2001. E-mail survey response rates: A review. *Journal of Computer Mediated Communication,* pp. 6(2):1-16.

Sherwood, J., Clark, A. & Lynas, D., 2009. *Enterprise Security Architecture,* USA: SABSA .

Sherwood, J., Clark, A. & Lynas, D., 2009. *Enterprise Security Architecture - SABSA,* USA: Sussex.

Singh, K., 2007. *Quantitative social research methods..* EBSCOHost ed. London: Sage .

Siponen, M. & Oinas-Kukkonen, H., 2007. A Review of Information Security Issues and Respective Research Contributions. *ACM SIGMIS Database,* 38(1), pp. 60-80.

Sivasubramaniyan, P., 2012. *Research Methodology: An Introduction,* s.l.: Lingaya Institute of Management and Technology.

Smith, M. & Erwin, J., 2005. *Role & Responsibility Charting (RACI),* s.l.: Project Management Forum.

SooHoo, K., 2000. *How Much Is Enough? A Risk-Management Approach to Computer Security..* s.l.:s.n.

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.* USA: Risk Management Guide for InformaNational Institute of Standards and Technology, Special Publication 800-30..

Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology ,* US: NIST Special Publication 800-30..

Straub, D., 2011. *Contemporary Black Hat, White Hat Research in Information Security: Where are the Gaps?,* s.l.: Penn State University, MIS Quarterly.

Susanto, H., Almunawar, M. & Tuan, Y., 2012. 91. Susanto H., Almunawar M., Tuan Y., 2012 January, Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level. *International Journal of Engineering and Technology ,* 2(1).

Swiderski, F. & Snyder, W., 2004. *Threat Modeling,* s.l.: Microsoft Press.

Swiderski, F. & Snyder, W., 2004. *Threat Modeling,* USA: Microsoft Press.

Tang-Jing & Shen-LePing, 2010. *The Risk Control Model in Corporate Governance – Based on Conditional Random Fields Based Security Risk Evaluation for IT Systems,* s.l.: IEEE.

Taylor, A., Alexander, D., Finch, A. & Sutton, D., 2008. Information Security Management Principles - An ISEB Certificate. In: T. B. C. Society, ed. s.l.:ISBN978-1-902505-90-9, pp. 1-37.

Trobia, A., 2008. Questionnaire. Encyclopedia of Survey Research Methods. In: s.l.:SAGE, pp. 653-656.

Trochim, W., 2006. *Research Methods Knowledge Base.* [Online] Available at: http://www.socialresearchmethods.net [Accessed 25 October 2014].

Utin, D., Utin, M. & Utin, J., 2008. General Misconceptions about Information Security Lead to an Insecure World. *Information Security Journal, A Global Perspective,* 14(4), pp. 164-169.

Uzunov, A. & Fernandez, E., 2013. *An Extensible Pattern-based Library and Taxonomy of Security Threats for Distributed Systems,* s.l.: Elsevier.

Van_der_Leeden, K., 2010. *Security without Risk? Investigating information security among Dutch universities.* Netherlands: University of Twente..

VanCleeff, A., 2010. *A Risk Management Process for Consumers: The Next Step in Information Security. NSPW'10..* Massachusetts, USA, ACM.

VanHorne, P., Olson, K. & Miller, K., 2001. *Automatic Static to Dynamic IP address and DNS address Management for Remote Communications Network Access,* USA: Cisco Technology Inc.

Verheul, E., 2011. *Practical implementation of ISO 27001 / 27002: Security in organisations,* s.l.: Radboud Universiteit Nijmegen:Digital Security Group.

VonSolms, B., 2001. Information Security – A Multidimensional Discipline. *Computers & Security,* 20(6), pp. 504-508.

VonSolms, B., 2005. *Information Security Governance: COBIT or ISO 17799 or both?,* s.l.: Elsevier.

VonSolms, R. & VonSolms, B., 2006. *Information Security Governance: A model based on the Direct-Control Cycle,* s.l.: Elsevier.

Walser, K., Kühn, A. & Riedl, R., 2009. *RISK MANAGEMENT IN E-GOVERNMENT FROM THE PERSPECTIVE OF IT GOVERNANCE.* USA, ACM, pp. 315-316 .

Walser, K., Kühn, A. & Riedl, R., 2009. *RISK MANAGEMENT IN E-GOVERNMENT FROM THE PERSPECTIVE OF IT GOVERNANCE.* s.l., The Proceedings of the 10th International Digital Government Research Conference.

Webb, J., Ahmad, A., Maynard, S. & Shanks, G., 2014. *A situation awareness model for information security risk management ,* s.l.: ScienceDirect, Computers & SecurityElsevier Ltd.

Weber, R., 2004. *The Rhetoric of Positivism versus Interpretivism,* s.l.: MIS Quarterly 28 (1) .

WebFinanceInc, 2010. *Business Dictionary.* [Online] [Accessed 15 January 2014].

White, M., 2012. *OCTAVE,* Pennsylvania: Indiana University of Pennsylvania: Eberly College of Business and Information Technology - Management Information Systems and Decision Sciences.

Whitman, M. & Mattord, H., 2005. *Principles of Information Security.* 2nd ed. s.l.:Thomson Course Technology.

Whitman, M. & Mattord, H., 2005. *Readings and Cases in the Management of Information Security,* Boston: ISBN0-619-21631-X.

Winter, R. & Schelp, J., 2008. *Enterprise Architecture Governance: The Need for a Business-to-IT Approach.* New York, USA, SAC '08 Proceedings of the 2008 ACM symposium on Applied computing, pp. 548-552 .

Winter, R. & Schelp, J., 2008. *Enterprise Architecture Governance: The Need for a Business-to-IT Approach,* s.l.: ACM: p548 – p552..

Yin, R., 2002. *Case Study Research, Design and Methods.* 3rd ed. Newbury Park: SAGE.

Yin, R., 2003. Case study research: Design and methods 3rd edition. In: T. Oaks, ed. CA: SAGE, pp. 14-19.

Zachman, J., 2011. *The Zachman Framework for Enterprise Architecture: The Enterprise Ontology,* USA: Zachman International.

Zhang, S. & LeFever, H., 2013. An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics, Business Management,* 1(4), pp. 391-395.

APPENDICES

8. APPENDIX A: SURVEY INVITATION LETTER

Dear Respondent,

You are humbly invited to participate in an academic research study which is conducted under the School of Computing, of the University of South Africa.

The purpose of this study is to investigate if the existing best practice IT security frameworks and standards can be unified to provide a more effective approach to management of both known and unknown IT security risks within a dynamic environment.

Responding to the questionnaire requires only your personal, professional experience and not that of the organisation that you work for. I confirm that all responses will be treated as strictly confidential and that anonymity will be ensured.

I value your participation and would appreciate it if you can complete this questionnaire. The questionnaire should not take more than 15 minutes of your time. Participation is voluntary and you are free to withdraw from this research at any time without any negative consequences.

Research Title:	A risk based approach for managing Information Technology security risk within a dynamic environment
Researcher:	Bessy Mahopo (née Gomba), MSc student, UNISA Email: 49020056@mylife.unisa.ac.za
Supervisor:	H. Abdullah GJ Gerwel Building, C4-62, Florida Campus, UNISA Email: abdulh@unisa.ac.za

Best Regards,
Bessy Mahopo

9. APPENDIX B: ETHICAL CLEARANCE

UNISA | college of science, engineering and technology

Ms Ntombizodwa Bessy Gomba (4920056) 2014-09-09
College of Science, Engineering and Technology
UNISA
Johannesburg

Permission to conduct research project

Ref: 165/NBG/2014

The request for ethical approval for your MSc (Computing) research project entitled "A risk based approach for managing information technology (IT) security risk within a dynamic environment" refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

Prof Ernest Mnkandla
Chair: College of Science, Engineering and Technology Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
The Science Campus
C/o Christiaan de Wet Road and Pioneer Avenue,
Florida Park, Roodepoort
Private Bag X6, Florida, 1710
www.unisa.ac.za/cset

UNISA | college of science, engineering and technology

10. APPENDIX C: SURVEY QUESTIONNAIRE

Questionnaire

Introduction:

The rapid growth of society's dependence on Information Technology (IT) has precipitated a growing apprehension about the security and reliability of this fragile infrastructure. Organisations and individuals always find themselves under pressure to stay abreast with the current technology in order to run their organisations or their lives, whereby their IT systems are open to the Internet. There is a tremendous amount of innovation involved with technology, which introduces a great deal of complexity within the IT environment, resulting in a significant number of IT security risks. Unfortunately, several issues remain unsolved including the need for sophisticated formalisation in the risk management reasoning, which is the basis of this research study.

The intention of this questionnaire is to assess if the proposed risk based approach would assist in managing IT security risk more proactively and more effectively in a dynamic environment.

This questionnaire is divided into the following sections:

Section 1: General Information about the respondent and their professional experience
Section 2: Best practice risk management frameworks and standards for IT security
Section 3: Approach to IT security
Section 4: Primary principles of the proposed IT security risk management approach

Notes and Instructions:

The questionnaire will take approximately 12 minutes to complete.

All questions relate to assessing if the proposed approach would be effective and efficient in addressing both known and unknown IT security risks within a dynamic environment.

Responding to the questionnaire requires only your personal, professional experience and not that of the organisation that you work for.

All responses will be treated as strictly confidential and anonymity will be ensured.

All questions are closed-ended.

Participation is voluntary and you are free to withdraw from this research at any time without any negative consequences.

SECTION 1: General information

Question 1

What is the size of the organisation that you work for?		
Small (< 200 Employees)	Medium (200-1 000 Employees)	Large (> 1 000 Employees)

Question 2

Does your day-to-day responsibility include management of IT security risk?	
Yes	No

Question 3

Which area of IT security are you involved in?			
Governance	Risk	Operations	Other _____

Question 4

Experience in IT Security?		
0-5 Years	6-10 Years	10 Years+

SECTION 2: Best practice risk management frameworks and standards for IT security

Question 5

The following scale will be used to indicate your opinion on the IT security risk management frameworks and standards used in defining the proposed approach:

Scale Value	Scale Description
1	Strongly Disagree: Indicates that the framework presented certainly does not assist in managing IT security risk.
2	Disagree: Indicates that the framework presented probably does not assist in managing IT security risk.
3	Neither Agree nor Disagree: Indicates that the respondent does not have a viewpoint about the presented framework.
4	Agree: Indicates that the framework presented does assist in managing IT security risk to some level if applied correctly.
5	Strongly Agree: Indicates that the framework presented certainly does assist in managing IT security risk if applied correctly.

Question 5(a)

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 5(b)

ISO 27001/2 (Information Security Standard)				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 5(c)

COBIT (Control Objectives for Information and Related Technology)				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 5(d)

ITIL (Information Technology Infrastructure Library)				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 5(e)

ISF (Standard of Good Practice for Information Security)				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

SECTION 3: Approach to IT Security

Question 6

The following scale will be used to indicate your opinion on the primary attributes of the proposed approach:

Scale Value	Scale Description
1	Strongly Disagree: Indicates that the principle presented by the statement certainly does not have an influence on the proactiveness and effectiveness of an IT security risk management approach.

2	Disagree: Indicates that the principle presented by the statement probably does not have an influence on the proactiveness and effectiveness of an IT security risk management approach.
3	Neither Agree nor Disagree: Indicates that the respondent does not agree nor disagree with the principle presented by the statement.
4	Agree: Indicates that the principle presented by the statement does have some level of influence on the proactiveness and effectiveness of an IT security risk management approach.
5	Strongly Agree: Indicates that the principle presented by the statement certainly has an influence on the proactiveness and effectiveness of an IT security risk management approach.

Question 6(a)

Use of a mix of top-down and bottom-up approaches to identify IT security risk				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 6(b)

Use of an iterative process for an IT security risk management approach				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 6(c)

Responsibility assignment (e.g. RACI model) for an IT security risk management approach				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 6(d)

Definition of input and output elements for an IT security risk management approach				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 6(e)

Inclusion of threat modelling to increase dynamicity of the IT security risk management approach				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

SECTION 4: Key principles of the proposed IT security risk management approach

Question 7

The following scale will be used to indicate your opinion on the key elements of the proposed approach:

Scale Value	Scale Description
1	Strongly Disagree: Indicates that the principle presented by the statement certainly does not have an influence on the proactiveness and effectiveness of

	an IT security risk management approach.
2	Disagree: Indicates that the principle presented by the statement probably does not have an influence on the proactiveness and effectiveness of an IT security risk management approach.
3	Neither Agree nor Disagree: Indicates that the respondent does not agree nor disagree with the principle presented by the statement.
4	Agree: Indicates that the principle presented by the statement does have some level of influence on the proactiveness and effectiveness of an IT security risk management approach.
5	Strongly Agree: Indicates that the principle presented by the statement certainly has influence on the proactiveness and effectiveness of an IT security risk management approach.

Question 7(a)

Organisational strategy and IT strategy as input elements for an IT security risk strategy				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(b)

Consideration of previous IT security risks and incidents for IT security risk identification				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(c)

Consideration of previous IT security audit findings for IT security risk identification				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(d)

Formal, periodic (e.g. quarterly) workshops for IT security risk assessments				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(e)

Threat modelling (IT security) at a business unit level at least once a year				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(f)

Development of an IT security risk register that is reviewed at least once a month				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

Question 7(g)

Formal communication (i.e. reporting) of IT security risk to senior management on a quarterly basis				
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

11. APPENDIX D: LANGUAGE EDITING

DECLARATION BY LANGUAGE EDITOR

20 November 2015

TO WHOM IT MAY CONCERN

DECLARATION: LANGUAGE EDITING of MSc Dissertation

I hereby declare that I have edited the Master of Science (in Computing) dissertation of NTOMBIZODWA BESSY MAHOPO entitled *"**A RISK-BASED APPROACH FOR MANAGING INFORMATION TECHNOLOGY SECURITY RISK WITHIN A DYNAMIC ENVIRONMENT**"* and found the written work to be free of ambiguity and obvious errors. It is the responsibility of the student to address any comments from the editor or supervisor. Additionally, it is the final responsibility of the student to make sure of the correctness of the dissertation.

Khomotso Bopape

Full Member of the Professional Editors' Guild

Professional EDITORS' Guild

Let's Edit is a Level 1 EME B-BBEE Contributor (Procurement Recognition Level = 135%)

Address: **P.O. Box 40208, Arcadia, Pretoria, 0007**
Tel No.: **012 753 3670,** Fax No.: **086 267 2164** and Email Address: **khomotso@letsedit.co.za**